

**Cyber-Activists as Innovators:
Online Technologies and the Power Struggle in Iran**

ARASH ANGHAEI

**A thesis submitted in partial fulfilment of the requirements of the University
of East London for the degree of Doctor of Philosophy**

July 2016

Abstract

This thesis analyses key social and technical capabilities and functions in Iran through the lens of the National Innovation System (NIS) model, focusing on processes influencing the on-going online encounter between the regime and local and expatriate pro-democracy cyber-activists in the aftermath of the country's contested presidential elections in June 2009. Conceptually, it is located in Science and Technology Studies (STS), with an emphasis on constructivist theory including Social Shaping of Technology (SST) as its creative backbone.

In the original Nordic conceptualisation of the NIS model, openness is considered a given. This prevents the model from adequately explaining the dynamics of innovation in repressive countries. In Iran, nationwide innovation processes are distorted by high level security officials' ideology-driven approach to the generation and diffusion of scientific knowledge and the influence of the Islamic Revolutionary Guards Corps (IRGC) over Iran's national economy. Bifurcated due to significant political differences, the Iranian NIS has become dysfunctional in the absence of an integrated, democratic structure, making the country highly dependent on foreign expertise.

The overreliance of Iran on cross-border technological contributions is reflected in the state's internet surveillance apparatus. Currently, major European information and communications technology (ICT) companies aid the core of the censorship infrastructure employed by the Iranian regime, while a great majority of the anti-filtering software used by the cyber-activists is developed by North American universities, research centres and human rights NGOs. This, in turn, highlights a limitation in the EU export policy regimen, which fails to promote the development of pro-democracy online innovations and remains relatively weak in terms of its ability to regulate the overseas trade of telecommunications technologies.

Laying emphasis on the social responsibility of large international telecommunications companies based on the outcome of a combination of weblog content analysis, semi-structured expert interviews and document reviews, the results of this project are expected to help improve Western policies on dual-use ICT exports to repressive countries. A focused attempt at the dynamisation of relevant legislation by the European Parliament (EP) can help more effectively foster egalitarian values in emerging economies through supporting legitimate, bottom-up dissent.

The main body of data used by this research was collected through a longitudinal observation of 65 Persian activist weblogs evaluated against an inductively crafted checklist. The preliminary findings of the weblog content analysis were later on examined in relation to the scripts of direct discussions with 17 active scholars and practitioners sampled largely by snowballing, as well as to an extensive archive of legal and journalistic documents.

TABLE OF CONTENTS

<u>CHAPTER i: INTRODUCTION</u>	1
<u>PREFACE</u>	1
<u>INTELLECTUAL INSPIRATIONS</u>	1
<u>AIMS AND OBJECTIVES</u>	2
<u>HYPOTHESIS AND KEY RESEARCH QUESTIONS</u>	2
<u>STATEMENT OF ORIGINALITY</u>	3
<u>IRAN'S GREEN MOVEMENT: POLITICAL ACTIVISM AND THE DIGITALISATION OF A CONFLICT</u>	3
<u>REVOLUTIONARY GUARDS GO DIGITAL: EXPLOITING ICTs TO CONFRONT POPULAR RESISTANCE</u>	5
<u>TECHNOLOGICAL DIPLOMACY: WESTERN POLICIES, THE IRANIAN DIASPORA AND THE INNOVATION CYCLE IN REPRESSIVE COUNTRIES</u>	6
 <u>CHAPTER ii: ONLINE TECHNOLOGIES, HUMAN CHOICES AND THE ONGOING E-STRUGGLE IN IRAN: SOCIAL SHAPING OF TECHNOLOGY MEETS NATIONAL INNOVATION SYSTEM</u>	8
 <u>STS AS A NEW MAINSTREAM PARADIGM: HUMAN AGENCY, ARTEFACT TRAJECTORY AND THE COMPLEX NATURE OF INNOVATION</u>	8
<u>TECHNOLOGICAL DETERMINISM, SOCIAL BIAS AND THE HUMANITARIAN SIGNIFICANCE OF THE CONSTRUCTIVIST RESPONSE: AN IS PERSPECTIVE</u>	9
<u>CYBER-ACTIVISM, MODERN SOCIAL MOVEMENTS AND ADVANCED ICTs' PATTERNS OF CREATION AND USE IN REPRESSIVE CONTEXTS</u>	10
<u>NATIONAL INNOVATION SYSTEM: THEORY AND PRACTICE</u>	12
<u>NIS FUNCTIONALITY: FROM NORDICA'S ORDINARY CHOICE TO THE DEVELOPING WORLD'S ULTIMATE DREAM</u>	15
<u>NIS IN EMERGING ECONOMIES: THEORETICAL GAPS IN THE LITERATURE</u>	16
<u>NIS VARIATIONS, INDIGENOUS TECHNOLOGY AND CROSS-BORDER DEPENDENCY: WHAT MAKES INNOVATIONS SOCIALLY SUSTAINABLE?</u>	18
<u>IRAN'S NIS: AN EMPIRICAL ANALYSIS OF A BIFURCATED STRUCTURE</u>	19
<u>NIS DYSFUNCTIONALITY IN IRAN AND THE COUNTRY'S INEVITABLE RELIANCE ON FOREIGN ICTs</u>	28
<u>CYBER-ACTIVISM: WHY FOCUS ON INNOVATION?</u>	36
 <u>CHAPTER iii: WEBLOG CONTENT ANALYSIS, EXPERT INTERVIEWS AND DOCUMENT REVIEW—A METHODOLOGICAL APPROACH DESIGNED FOR REPRESSIVE CONTEXTS</u>	38
 <u>METHODOLOGICAL DILEMMAS: COMPASSION, DETACHMENT AND SELF-REFLEXIVITY IN SOCIAL RESEARCH</u>	38
<u>ACTIVIST RESEARCH SERVING SOCIAL SCIENCES: BRIDGING THE GAP BETWEEN THEORY AND PRACTICE IN STS</u>	39
<u>HINDSIGHT REFLECTIONS: DECONSTRUCTING THE RESEARCH DESIGN IN RETROSPECT</u>	43
<u>RESEARCH METHODS: AN OVERVIEW</u>	44

<u>WEBLOG CONTENT ANALYSIS</u>	45
<u>EXPERT INTERVIEWS</u>	48
<u>DOCUMENT REVIEW</u>	50
<u>ANALYTICAL FRAMEWORK</u>	50
<u>ETHICAL CLEARANCE</u>	51
 <u>CHAPTER iv: DEMOCRATIC STRUCTURE, BIMODALITY AND NIS—A TRIANGULATED ANALYSIS OF THE INNOVATION PATTERNS AND PROCESSES WITHIN IRAN'S ONLINE SPHERE</u>	53
 <u>ACTIVISM IN IRAN: WHERE DO ICTs STAND?</u>	53
<u>ANTI-CENSORSHIP INNOVATIONS: HOW DO THEY EMERGE?</u>	56
<u>CYBER POLICE, ONLINE ACTIVISTS AND SELF-RELIANCE IN THE VIRTUAL POWER STRUGGLE IN IRAN</u>	65
<u>WESTERN ICTs VS. LOCAL POLITICS: EUROPEAN INNOVATIONS AND THE DYNAMICS OF ONLINE CENSORSHIP IN IRAN</u>	71
<u>IRGC, NATIONWIDE INNOVATION PROCESSES AND THE BREAKDOWN OF IRAN'S NIS</u>	75
<u>CYBER-ACTIVISM, NETWORK LITERACY AND THE INNOVATION OF CHANGE</u>	87
<u>MAPPING THE GEOGRAPHY OF CYBER-ACTIVISM IN IRAN: COUNTER-CENSORSHIP INNOVATIONS AND THE LOCAL/EXPATRIATE DIVIDE</u>	90
<u>NETWORK ACCESS, COMPUTER LITERACY AND ONLINE INNOVATIONS: GENDER EQUALITY AS A CATALYST OF CHANGE</u>	97
<u>GENDER, DEMOCRATIC LEGITIMACY AND INNOVATION: A SOCIOLOGICAL APPROACH TO CYBER-ACTIVISM IN IRAN</u>	97
<u>LEGISLATIVE POWERS OF THE EUROPEAN PARLIAMENT: POLICY AS A PREVENTATIVE MEASURE</u>	104
<u>TELECOMMUNICATIONS TECHNOLOGIES, ETHICAL VALUES AND INTERNATIONAL TRADE POLICIES: TOWARDS A COMPREHENSIVE EUROPEAN FRAMEWORK</u>	107
 <u>CHAPTER v: UKRAINE, CHINA AND THE ARAB SPRING: CYBER-ACTIVISM AND THE TECHNO-UTOPIAN SEARCH FOR A UNIVERSALLY TRANSFERABLE MODEL OF DEMOCRATIC CHANGE</u>	109
 <u>UKRAINE'S ORANGE MOVEMENT: LESSONS IN E-REVOLUTION</u>	109
<u>ARAB SPRING: DAWN OF A REVOLUTIONARY MODEL OR DUSK OF A TECHNO-UTOPIAN DREAM?</u>	116
<u>HI-TECH TELECOMMUNICATIONS, POLITICAL OPENNESS AND SECURITY INITIATIVES: THE CASE OF POST-REFORM CHINA</u>	119
 <u>CHAPTER vi: FOSTERING DEMOCRACY—WESTERN EXPORT CONTROL REGIMES, CORPORATE SOCIAL RESPONSIBILITY AND THE TECHNOLOGY OF REPRESSION</u>	122
 <u>TRADE REGULATION, WESTERN POLICIES AND POWER STRUGGLES IN REPRESSIVE STATES</u>	122
<u>CASE STUDY: NOKIA-SIEMENS NETWORKS AND THE IRANIAN MARKET</u>	124
<u>NSN AND POLICY LESSONS FOR THE FUTURE: AN ANALYSIS</u>	124
<u>ANTI-CENSORSHIP TECHNOLOGY: FOSTERING DEMOCRACY IN A CONVERGING WORLD</u>	128
<u>HACKTIVISM AND INNOVATION: THE BLURRED LINES OF ONLINE DISSENT</u>	132

CHAPTER vii: CONCLUSIONS, PRACTICAL IMPLICATIONS AND INSIGHTS FOR FUTURE RESEARCH..... 136

<i><u>OUTRIGHT BIMODALITY VS. LIMITED DIFFUSION: CAN A SINGLE NIS SERVE TWO DIFFERENT MASTERS?</u></i>	136
<i><u>IRGC GENERALS AND THE MILITARISATION OF IRAN'S CIVIL INDUSTRIES: THE BIRTH OF A DYSFUNCTIONAL SYSTEM</u></i>	138
<i><u>WHY DEMOCRACY MATTERS: THE SOCIAL STRUCTURE OF AN NIS AND ITS TECHNICAL POTENCY....</u></i>	139
<i><u>IN SEARCH OF A CROSS-BORDER MODEL FOR DEMOCRATIC CHANGE: A UNIVERSALLY TRANSFERRABLE NIS?</u></i>	143
<i><u>INNOVATION PROCESSES AND POLITICAL MOVEMENTS: IDEAS FOR FUTURE RESEARCH</u></i>	146

REFERENCE LIST..... 148

APPENDICES.... 197

<i><u>ETHICS APPROVAL CERTIFICATE</u></i>	198
<i><u>BLOG CONTENT ANALYSIS DOCUMENTS</u></i>	200
<i><u>Blog Analysis Questions</u></i>	201
<i><u>Analysed Blogs</u></i>	201
<i><u>INTERVIEW SCRIPTS</u></i>	228
<i><u>Dr. Alexander Dawoody (31 Aug 2012)</u></i>	229
<i><u>Dr. Babak Rahimi (30 Aug 2012)</u></i>	233
<i><u>Elahe Boghrat (13 Sep 2012)</u></i>	235
<i><u>Dr. James Fielder (30 Aug 2012)</u></i>	238
<i><u>Dr. Jed Crandall (03 Sep 2012)</u></i>	241
<i><u>Kevin G. Coleman (04 Sep 2012)</u></i>	243
<i><u>Layla Hashemi (31 Aug 2012)</u></i>	245
<i><u>Madeline Storck (03 Sep 2012)</u></i>	248
<i><u>Dr. Marcus Michaelsen (30 Aug 2012)</u></i>	250
<i><u>Dr. Nassim Nazemi (09 Oct 2012)</u></i>	251
<i><u>Neal Ungerleider (21 Sep 2012)</u></i>	253
<i><u>Prof. Paul Holman (23 Sep 2012)</u></i>	255
<i><u>Pejman Akbarzadeh (03 Sep 2012)</u></i>	256
<i><u>Dr. Randy Kluver (30 Aug 2012)</u></i>	258
<i><u>Dr. Soheila Vahdati-Bana (04 Sep 2012)</u></i>	260
<i><u>Dr. Tessa Houghton (14 Sep 2012)</u></i>	261
<i><u>Dr. Ulises Mejias (24 Sep 2012)</u></i>	263
<i><u>WESTERN TECHNOLOGY EXPORT CONTROL POLICY REFERENCES</u></i>	265
<i><u>EU</u></i>	266
<i><u>UN</u></i>	267
<i><u>US</u></i>	268

GLOSSARY OF TERMS..... 269

Figures

<u>FIGURE 1. IRANIAN REGIME AND THE TECHNOLOGIES OF MASS DESTRUCTION</u>	<u>20</u>
<u>FIGURE 2. THE HIERARCHY OF THE IRANIAN REGIME</u>	<u>22</u>
<u>FIGURE 3. A SATELLITE SIGNAL JAMMING MACHINE INSTALLED BY THE IRANIAN AUTHORITIES.....</u>	<u>22</u>
<u>FIGURE 4. OIL INCOME AND THE IRANIAN NIS.....</u>	<u>25</u>
<u>FIGURE 5. LUNDVALL'S CYCLE OF INNOVATION.....</u>	<u>25</u>
<u>FIGURE 6. INHIBITIONS AND BARRIERS TO THE IRANIAN NIS.....</u>	<u>26</u>
<u>FIGURE 7. TRIPLE HELIX MODEL.....</u>	<u>27</u>
<u>FIGURE 8. REGIME'S INNOVATION SYSTEM IN IRAN.....</u>	<u>28</u>
<u>FIGURE 9. AUTHORITARIAN VS. CIVILIAN TECHNOLOGY ADVANTAGE.....</u>	<u>33</u>
<u>FIGURE 10. FOREIGN TECHNOLOGIES, IRGC AND THE ONLINE POWER STRUGGLE IN IRAN.....</u>	<u>34</u>
<u>FIGURE 11. INTERNET CENSORSHIP TECHNOLOGIES: COST-EFFECTIVENESS VS. ACCURACY</u>	<u>35</u>
<u>FIGURE 12. RESEARCH METHODS: A TAILORED DESIGN FOR A REPRESSIVE CONTEXT.....</u>	<u>45</u>
<u>FIGURE 13. EXPERT SURVEY: THE SIGNIFICANCE OF ONLINE TECHNOLOGY TO POLITICAL ACTIVISM IN IRAN.....</u>	<u>54</u>
<u>FIGURE 14. TWITTER: POLITICALLY MOTIVATED HACKING ATTACKS GO VIRAL.....</u>	<u>59</u>
<u>FIGURE 15. GOOGLE CHROME: SSL CONNECTION ERROR.....</u>	<u>60</u>
<u>FIGURE 16. CENSORSHIP SNIFFER: IS 'THIS' BLOCKED IN IRAN?</u>	<u>60</u>
<u>FIGURE 17. EXPERT SURVEY: THE COMMONNESS AND PRACTICALITY OF CONVENTIONAL ANTI-CENSORSHIP TECHNOLOGIES IN IRAN</u>	<u>61</u>
<u>FIGURE 18. PIRATEBROWSER: OPEN SOURCE PROGRAMMING AT COUNTER-CENSORSHIP SERVICE....</u>	<u>63</u>
<u>FIGURE 19. LIMEWIRE: PEER-TO-PEER NETWORKING TO FIGHT ONLINE CENSORSHIP</u>	<u>63</u>
<u>FIGURE 20. FOREIGN EMPATHY AND INTERNET CENSORSHIP IN IRAN.....</u>	<u>65</u>
<u>FIGURE 21. ACCESS FLICKR: HOME-GROWN ANTI-CENSORSHIP SOFTWARE IN ACTION</u>	<u>65</u>
<u>FIGURE 22. GREEN PROXY: BREAKING THROUGH INNOVATION BARRIERS.....</u>	<u>66</u>
<u>FIGURE 23. GREEN PHOENIX: ENDOGENOUS, FUNCTIONAL AND POPULAR</u>	<u>67</u>
<u>FIGURE 24. EXPERT SURVEY: THE REGIME'S DEGREE OF SELF-EFFICACY IN CYBER CENSORSHIP.....</u>	<u>67</u>
<u>FIGURE 25. EXPERT SURVEY: THE CONTRIBUTION OF EUROPEAN-SOURCED TECHNOLOGIES TO ONLINE POWER STRUGGLES IN IRAN.....</u>	<u>71</u>
<u>FIGURE 26. IRAN'S NIS, DUAL-USE ICTS AND THE EU/US EXPORT POLICY DIVIDE.....</u>	<u>74</u>
<u>FIGURE 27. TECHNOLOGY DEVELOPMENT AND INTERSECTIONAL COOPERATION: MILITARY VS. CIVILIAN.....</u>	<u>75</u>
<u>FIGURE 28. TECHNOLOGY IMPORTS, IRGC AND THE MILITARY/CIVILIAN DYNAMICS OF INNOVATION IN IRAN.....</u>	<u>75</u>
<u>FIGURE 29. ACCESS DENIED: DCI AND INTERNET CENSORSHIP IN IRAN.....</u>	<u>78</u>
<u>FIGURE 30. BLOG CONTENT ANALYSIS: COMPUTER LITERACY & IRANIAN CYBER-ACTIVISTS</u>	<u>89</u>
<u>FIGURE 31. BLOG CONTENT ANALYSIS: GEOGRAPHICAL LOCATION & IRANIAN CYBER-ACTIVISTS.....</u>	<u>93</u>
<u>FIGURE 32. BLOG CONTENT ANALYSIS: GEOGRAPHICAL LOCATION OF EXPATRIATE IRANIAN CYBER-ACTIVISTS.....</u>	<u>94</u>
<u>FIGURE 33. WOMEN AND HIGHER EDUCATION: A WORLDWIDE COMPARISON.....</u>	<u>103</u>
<u>FIGURE 34. EXPERT SURVEY: THE CAPACITY OF THE EUROPEAN PARLIAMENT TO ADDRESS ONLINE CENSORSHIP IN IRAN.....</u>	<u>104</u>
<u>FIGURE 35. ANTI-CENSORSHIP TECHNOLOGIES: ONE SIZE DOES NOT FIT ALL.....</u>	<u>131</u>
<u>FIGURE 36. TWITTER: DDoS ATTACKS GO VIRAL.....</u>	<u>133</u>

Tables

<u>TABLE 1. ORGANISATIONAL VALUES: MILITARY VS. ACADEMIA</u>	<u>30</u>
<u>TABLE 2. FILTERING SOFTWARE AND DATABASE COMPILATION</u>	<u>36</u>
<u>TABLE 3. BLOG ANALYSIS CHECKLIST</u>	<u>48</u>
<u>TABLE 4. INTERVIEW QUESTIONS</u>	<u>50</u>
<u>TABLE 5. EXPERT INTERVIEWS: THE SELF-EFFICACY OF THE IRANIAN REGIME'S CURRENT ONLINE CENSORSHIP SYSTEM</u>	<u>70</u>
<u>TABLE 6. FOREIGN ICTS AND ONLINE CENSORSHIP IN IRAN</u>	<u>73</u>
<u>TABLE 7. NORTH AMERICA AND THE EMERGENCE OF COUNTER-CENSORSHIP TECHNOLOGIES.....</u>	<u>73</u>
<u>TABLE 8. VALIDATING THE RESULTS: A THREE-DIMENSIONAL ANALYSIS.....</u>	<u>81</u>
<u>TABLE 9. CONCLUDING THE RESEARCH: HYPOTHESIS REVISITED.....</u>	<u>81</u>
<u>TABLE 10. PERSIAN BLOGGERS, COMPUTER LITERACY AND INNOVATIVE USE OF ONLINE TECHNOLOGIES</u>	<u>89</u>
<u>TABLE 11. PERSIAN BLOGGERS: THE GEOGRAPHY OF ONLINE DISSENT.....</u>	<u>93</u>
<u>TABLE 12. GENDER INEQUALITY INDEX: 2008 VS. 2011.....</u>	<u>98</u>
<u>TABLE 13. GLOBAL GENDER GAP REPORT 2009.....</u>	<u>99</u>
<u>TABLE 14. HUMAN DEVELOPMENT INDEX 2011.....</u>	<u>99</u>
<u>TABLE 15. PERSIAN BLOGGERS: GENDER AND CYBER-ACTIVISM IN IRAN.....</u>	<u>102</u>
<u>TABLE 16. IRAN'S INTERNET FREEDOM STATUS.....</u>	<u>104</u>
<u>TABLE 17. UKRAINIAN DISSIDENTS AND INTERNET LITERACY.....</u>	<u>111</u>
<u>TABLE 18. IMPLICATIONS OF 'ANTI-PIRACY' POLICIES: WESTERN DEMOCRACIES VS. REPRESSIVE STATES.....</u>	<u>124</u>
<u>TABLE 19. UNITED STATES CONGRESS AND ANTI-CENSORSHIP TECHNOLOGIES.....</u>	<u>129</u>
<u>TABLE 20. COMMON WAYS TO BYPASS INTERNET CENSORSHIP.....</u>	<u>130</u>
<u>TABLE 21. ANTI-CENSORSHIP SOFTWARE: A COMPARATIVE EVALUATION.....</u>	<u>130</u>
<u>TABLE 22. WORLD'S TOP CYBER POWERS UNDER SCRUTINY</u>	<u>134</u>

Abbreviations

Cyber-activist Innovation System (CIS) is a term coined by this research, which refers to an interconnected network of computer-literate, pro-democracy, online activists focused on counter-censorship ICT innovations.

Distributed Denial of Service (DDoS) describes ICT-based attacks aimed to make an online network temporarily inaccessible to its potential users.

Information and Communications Technology (ICT) refers mainly to the integration of traditional communication techniques with online networks through cabled or cable-free connections.

Innovation System (IS) refers to the systematic flow of information among actors needed in order to transform ideas into tangible results.

Iranian Cyber Police (FATA) is an online-oriented division of the Iranian police founded in January 2011.

Islamic Republic of Iran Broadcasting (IRIB) is a regime-subsidised Iranian corporation in control of all broadcast media.

Islamic Revolutionary Guard Corps (IRGC) is a giant, powerful organisation of nearly 130,000 specialised personnel and parallel to Iran's military, which specifically aims to ensure the compliance of all the regime's general endeavours with the teachings of Islam.

National Innovation System (NIS) refers to the flow of technological information among people, enterprises and institutions, the collaboration among which reflects a given country's innovation robustness and powers.

National Iranian Oil Company (NIOC) is a government-owned corporation run (and owned by) Iran's Oil & Petroleum Ministry.

Science, Technology and Society (STS) is the study of the interplay between socio-political (and sometimes cultural) values and technological innovations across one or more geographical regions.

Social Construction of Technology (SCOT) is an STS theory arguing against technological determinism, introducing technology as the ultimate product of human choices/actions.

Social Networking Services (SNSs) are online platforms aiming to enable conventional social relations among people favouring the same causes/interests.

Social Shaping of Technology (SST) is an STS model developed by MacKenzie and Wajcman in 1985 with a strong criticism of technological determinism, underlining the socio-political contexts influencing a nation's technological choices.

Sociology of Scientific Knowledge (SSK) is the study of the relationship between social processes and scientific activity.

Supreme Council of Cultural Revolution (SCCR) is a hard-line assembly based in the holy city of Qom, the main duty of which is ensuring full alignment of all cultural and educational productions and services with the core teachings of Islam and free from any Western influences.

Supreme Council of Cyberspace (SCC) is an assembly chaired by the Iranian president and responsible for regulating the online sphere.

Supreme National Security Council (SNSC) is a security-oriented, policy-focused assembly as demanded by the Islamic Republic's constitution, which aims to safeguard the regime in the matters of national security, defence and inland or foreign threats.

Acknowledgments

I would like to express my gratitude to Dr Josephine Stein, Professor Gavin Poynter and Dr Timothy Hall, without whose excellent supervision, this research would not have been possible.

This thesis is dedicated to my amazing parents Farideh and Mohsen, who have always supported me unconditionally and to the fullest.

Is a tractor bad? Is the power that turns the long furrows wrong? If this tractor were ours, it would be good—not mine, but ours. We could love that tractor then as we have loved this land when it was ours. But this tractor does two things—it turns the land and turns us off the land. There is little difference between this tractor and a tank. The people were driven, intimidated, hurt by both. We must think about this.
—John Steinbeck, *The Grapes of Wrath*, 1939



Preface

Digital technologies have been influencing social change in Iran since 2009. Following the physical oppression of the street protesters in the aftermath of the contested presidential elections in June 2009, there was a gradual boost in the politically motivated use of information and communications technologies (ICTs) within the opposition camp. This was immediately confronted by a drastic enhancement of online censorship by the relevant government agencies. Each party is driven to invest a great deal of resources in establishing a steady leverage in this potent online world. Every new technology implementation by the one is routinely met with the launch of a timely (though not necessarily indigenous) counter innovation by the other. This project has attempted to combine and apply the National Innovation System (NIS) and Social Shaping of Technology (SST) models, in a bid to explain the socio-technical dynamics behind online innovations in Iran. It has subsequently developed an analytical framework to help improve Western technology export policies useful for fostering democracy, as well as for the promotion of pro-democracy innovation, in Iran and in other repressive countries. The notions of democracy and repressiveness employed by this thesis have been constructed largely based on those argued by Arendt (1951) and Habermas (1994; 2006) respectively.

Intellectual Inspirations

This project has been inspired by the idea that identifying and explaining the weaknesses and vulnerabilities of a dysfunctional NIS, and the implications such flaws raise for Western policy development, can help democratically reform the political structure under which that NIS operates. I have chosen Iran as the main case study, due to my direct knowledge about the country and my ability to read Farsi.

Iran is not a democracy. A religious elite governs, imposing its ideologies on the rest of the society. Further, a vibrant pro-democracy current, Iran's Green Movement has, according to the Brooklyn Institute for Social Research (BISR) (2012), played a prominent role in inspiring successive pro-democracy protests in the Middle East, and thus deserves an in-depth scrutiny.

The correlation between online innovations and the dynamics of democratic transition in repressive states is underrepresented in the mainstream Science and Technology Studies (STS) literature. Conversely, while an array of largely techno-utopian arguments have been made by 'futurist' experts such as Pesce (2010) and technical journalists in publications like PCWorld, CNet and Engadget, not many reliable, scholarly conclusions have been reached to date. There are currently significant geographically patterned differences among researchers' intellectual focus in relation to the public use of ICTs. In Western, developed countries, the scope of socio-technical research is often limited to the efficiency of e-government attempts that affect the capacity of online technologies to enhance the level of interaction between the government and the citizens in an industrialised democracy. Meanwhile, sensationalist terms such as 'Twitter revolution' and 'Facebook revolution' have been an integral cog in the construction of a sort of 'cyberbole' in media accounts on the Middle Eastern and North African (MENA) revolts since the late-2000s. Journalistic coverage aside, a wealth of academic literature has been produced surrounding the subject over the same time period by

social scientists worldwide. These range from the highly sceptical critiques of 'solutionism' by Morozov (2011) and Veksler (2007) to the far more optimistic Cognitive Surplus theory of Shirky (2010) and the Make and Connect Agenda of Gauntlett (2011). But whose argument is based more on substantial evidence and/or proven theory? Currently, most of the research conducted in the field do not go beyond technologically deterministic assumptions, and have little or no consideration of the still under-theorised interplay between ICTs and power in autocracies.

Aims and Objectives

The aim of this research is to investigate the dynamics of innovation and how they influence the power struggle between the Iranian cyber-police and the country's online pro-democracy activists.

The main objective of this thesis is to explain the innovation processes used by the Iranian regime and the country's local and expatriate cyber-activists in order to identify the effectiveness of forces enabling repression, as well as those facilitating democracy. The results of this research will be relevant to the development of democratic discourse and the control of ICT-mediated repression.

Hypothesis and Key Research Questions

My hypothesis is that there are two separate systems of innovation in place in Iran, both of which are heavily reliant on foreign telecommunications technologies. I identify and describe these two separate systems and how they interrelate yet remain distinct. This continued separation is primarily due to the Iranian regime's focus on militaristic and ideological objectives, which distorts nationwide innovation processes, preventing the two systems from uniting and forming an integrated system that serves the public's legitimate needs and interests. I also propose that it is not this bimodality, but instead the systemic lack of a democratic structure within either culture, which lies behind the overall dysfunctionality of the country's NIS. While in both 'underdeveloped' and 'repressive' contexts there are practical barriers to communication amongst the main pillars of innovation, there is nothing actively preventing national linkages from being constructed, and from mutually learning, under democratic rule. In Iran's case, the IRGC plugs into academia through its elite military universities, failing at the same time to connect with other elements that are not under its direct, hegemonic control.

This project aims to address the following questions:

- 1) How do actors within the Iranian regime on the one hand and cyber-activists on the other exploit and develop online technologies in their conflicts with one another?
- 2) What are the capabilities and functionality of Iran's National Innovation System with regards to telecommunications technologies?
- 3) To what extent and why are imported ICTs used in the power struggle between the regime and the cyber-activists in Iran?

Statement of Originality

Since most of the scholarship in STS has been intellectually focused on the innovation processes in Western democracies, where the NIS theory best applies, not much attention has been paid to the socio-technical dynamics of ICT innovation in repressive countries. Using Iran as a case study, this research attempts to expand upon the mainstream NIS model in order to fill this theoretical gap.

Many analysts and commentators (Searls and Sifry 2003; Shirky 2010) have taken a technologically deterministic standpoint to the outcomes of ICT innovation, failing to take into account the socio-technical factors at work in repressive states. The journalism industry has not hesitated to reduce complex innovation processes to a passive response to a 'technology push,' proposing arguments not adequately justified from a scholarly perspective. This was all-too-familiar during Iran's post-election unrest in June 2009 as well as during the Arab Spring protests in 2010 and 2011, when articles and editorials with a techno-utopian bent dominated the news media and frequently appeared in such venues as *The Economist* and *The Daily Telegraph*, extolling the so-called 'liberating powers' of the internet. This study identifies substantial bias in most previous approaches to the issue, and develops a new model to more accurately explain the interplay between ICTs and democracy in autocratic countries.

Iran's Green Movement: Political Activism and the Digitalisation of a Conflict

Before we can proceed with a thorough analysis of ICT innovation processes in Iran, it is critical to fully understand the specific socio-political circumstances in which these processes are at play. What follows is a context-driven profile of Iran, with a distinct focus on the aftermath of the contested presidential elections in June 2009.

The intolerant approach to peaceful street protests employed by the Islamic Republic's top security officials caused mainstream political dissent to be diverted to the online sphere, especially as ICTs became increasingly embedded into the Iranian urban lifestyle. Millions of political dissidents intolerant of the continuing physical casualties channelled their way across to each other through the internet—a promising medium of communication customarily championed by popular media as a safe haven for oppositions of all kind. The significance of ICTs to sustaining Iran's Green Movement has been rarely contested. Golkar (2011: 56) explains that the regime's legitimacy was never seriously challenged until "the publication of reports and videos of rape inflicted by security forces on detainees, especially in Kahrizak prison, as a result [of which] some religious leaders, intellectuals and reformists harshly criticised the government." Among these was the late Ayatollah Hussein-Ali Montazeri, Iran's most prominent cleric dissident, who openly denounced the results of the 2009 presidential elections (McClatchy Newspapers 2009). Kurzman's (2012: 163) analysis of the leaked images of the protests suggest that "virtually every image of the Iranian Green Movement included, somewhere in the frame, a picture of someone taking a picture" using a camera phone. Assessments such as these, although useful in determining the involvement of digital technologies in the revolt under study, continue the discussion mostly at the techno-utopian level and are thus in need of further conceptual dynamisation.

Today, the direct, unmodified application of Western scholarly frameworks to repressive contexts remains a common problem in Social Sciences (Fu et al. 2013; Fuller 1995; Pattersson 1982). A brief examination of post-2009 mainstream politics in Iran, therefore, seems crucial to understanding the extent to which online technologies can influence the chosen context.

Despite the Islamic State's routine civil rights violations in the past, the crackdown on the 2009 protests distinctively marks the beginning of a new period in the relationship between the citizens and the state officials, one during which even the centrist layers of the society lost faith in the regime. Beeman (2009: 5) scrutinises the issue from a Social Contract Theory perspective, asserting that "by allowing—or even by some accounts ordering—the beating of women and young people, effecting house arrests and crackdowns, the authorities in Iran essentially broke their contract with the people. In both cases, social order began to fray." Ahmadi (2009: 7) considers the heavy-handed attacks on the pro-democracy opposition as "declaring a war on Iran's civil society forces . . . [alienating to the] majority of population, and significantly [radicalising to] the nonviolent movement." Kojoori-Saatchi's (2010: 105) study concluded with the view that the government's response to the demonstrations was surprisingly violent behaviour, which "took the absolutist nature of the regime too far." Alimardani's (2011: 7) investigation held the top Islamic Revolutionary Guards Corps (IRGC) generals directly responsible for putting the "clerical elite . . . at odds with the public's democratic aspirations." Finally, Paris (2011: 7) portrays Iran's 2009 presidential election as a turning point in the history of the Islamic revolution, during which the regime completely lost the only two sources of legitimacy it had always claimed to have: "The Iranian people, who saw their votes dismissed, and the religious establishment, many of whom lost confidence in the supreme leader after he lent his partisan support for President Ahmadinejad in the dispute over the election."

The disintegration of trust between the citizens and the regime in the face of the street crackdowns has transformed the nature of the relationship between political dissidents and the ruling elite from co-existence into a complete ideological collision. This is precisely the reason why the hard-line core of the regime reacted so impulsively to what was arguably just an electoral dispute. Zehforoush (2012: 1) notes a tendency within the neo-conservative strata to thoroughly cleanse the socio-political scene in Iran in its favour, explaining that "the concepts of revolution and revolutionism in general, and the 1979 Iranian revolution in particular, have been the first victims of this new thinking." This has been systematically countered by what Hakakian (2012) alleges to be the Iranian citizens' priority to escort the "clergy back to the mosque . . . [and] to stand on secular legs." Heideman (2009: 5), likewise, views the post-2009 oppositional current as a "non-violent and non-ideological pro-democracy movement which demands individual freedom and civil rights."

Non-violent movements do not often translate into a peaceful transition of power in repressive states. In the event of a political turmoil, telecommunications technologies do not function just as a reflection of democracy, but equally as a weapon helping the dominant force to avoid it. As the internet turns increasingly into a user-oriented technological tool that proportionally rewards innovativeness, autocratic regimes will continue to burst the technoutopian bubble, utilising the medium to defy what was once perceived by most to be its 'ultimate' purpose.

Revolutionary Guards Go Digital: Exploiting ICTs to Confront Popular Resistance

IRGC, the security arm of the Islamic Republic, has had a tangible online presence since the outbreak of the street protests in June 2009. Once considered to be a leisure time activity for the 'upper-class,' blogging and social networking have been transformed by political dissidents into an influential means of protest. Millions of Iranian citizens can be considered pro-democracy cyber-activists (Daily Aztec 2011). The Islamic regime is now ranked as the world's worst internet oppressor (OpenNet Initiative 2011a), while also boasting a potent, rapidly expanding cyber army (United States Institute of Peace 2013), making the country one of only five states with cyber warfare capabilities (Military Advantage 2008).

A major inadequacy in the scholarly community's response to the post-2009 political developments in Iran was its inability to avoid the temptation to hypothesise purely based on journalistic accounts by enthusiastic observers who gave precedence to recency over depth, evidentiary accuracy and clarity of analysis. This has led to a somewhat exaggerated description of the relation of internet and Web 2.0 applications with modern social movements in repressive countries, portraying telecommunications technologies as democratic in nature. Burns and Eltham (2009: 304) disapprove of this techno-utopian approach, calling for attention to the fate of the pro-democracy cyber-activists in Iran, many of whom received long prison sentences (CBS Interactive 2012) after the launch of Iran's cyber police in January 2011. They observed a commonly overlooked notion: the threats ICTs present for political activists. In their view, "social media became a vector for state repression . . . —a pattern in earlier unsuccessful revolutions." This is not to deny the mobilising capacities of the internet, but to suggest that ICTs are mostly non-partisan in nature, and that there are valuable technical lessons for any stakeholders involved in a modern power conflict, regardless of location or intent. According to Burns and Eltham (2009: 303), the Iranian protesters' use of social media platforms to challenge the regime validated "one of the theses of the revolution in military affairs: that activist movements would tap the internet for global reach." This, in turn, is precisely why repressive regimes almost always resort to 'pulling the plug' of the internet as an immediate sign of panic in the face of popular revolt (Aking et al. 2012; Arnaudo et al. 2013; Bowman and Camp 2013; Howard et al. 2011; Papic and Noonan 2011; Scott 2012; Yang 2013).

The IRGC's timely, scalable tap into the internet could indeed be considered to be the Islamic Republic's key to surviving the most challenging act of opposition in its history of existence (Moore and Selchow 2012; Mueller and Van Huellen 2012; Washington Times 2009a). Metghalchi (2011: 58) views IRGC's armed support as economically-driven and a major contributor to the endurance of the Islamic Republic despite the continued opposition, gradually transforming a semi-autocracy to an absolute military dictatorship. The IRGC "stood firmly behind Supreme Leader Khamenei . . . [who later that year awarded them] a majority stake in the state telecommunications company." The relationship between the neo-conservative core of the regime and IRGC's top generals is a mutually convenient one, whereupon they grant one another the much important support each requires, through a blatant exchange of money and power. Ahmadi (2009: 6) detects a rapidly growing military-intelligence coalition taking over key profitable businesses ranging from construction and automobile manufacturing to laser eye surgery and real estate. This arrangement has subsequently prepared the ground for the Ayatollahs to, as Clark (2011: 23) explains, "use state apparatuses against protesting citizens and political dissidents" during and after the 2009

street protests—simply investing communal resources (e.g. oil and gas revenues) into suppressing popular dissent.

The 'cat and mouse' nature of the online power struggle in Iran means that the mere existence of a computer-literate opposition can keep the oppressive force on guard and in need of frequent ICT developments, as any victory in such competitive settings is necessarily temporary and subject to successful challenge by the 'counter-innovators.' Posch (2010: 46) argues that dissent, no matter how weak or disorganised, effectively prevents the one process truly necessary for the Islamic regime in its pursuit of ideological Utopia—"the creation of a new fixed narrative and reading of the events that took place in 2009 in the Islamic Republic." Thus, the Iranian cyber-activists' contributions to Iran's political discourse is essential to the enhancement of democratic developments in the country, and one which can be equally strengthened or weakened via relevant Western policies to which it happens to be exposed.

Technological Diplomacy: Western Policies, the Iranian Diaspora and the Innovation Cycle in Repressive Countries

The influence of Western policy on the socio-technical developments in repressive countries is a largely underexplored subject. This theoretical gap not only persists in the literature but also directly contributes to the distortion of political developments in such states by: a) allowing dual-purpose Western ICTs to quietly find their way to security officials in repressive regimes, and b) depriving pro-democracy dissidents residing in emerging economies of effective access to their basic technological needs to battle online censorship.

While US politicians have been reasonably active in supervising dual-use ICT export to repressive countries like Iran, the EU seems to have viewed the legislative approach a little more sceptically, enabling the exposure of the world's largest trading block (Belward 2013; De Ville and Orbie 2013; Jørgensen 2013) to illegitimate end users. Ahmadi (2009: 7) sees a big role for the use of economic powers in the global promotion of democracy, suggesting that "unless the international community rejects the IRGC coup's legitimacy and puts significant pressure on the Iranian government to respect the rights of their citizens, the situation will further deteriorate." Also, Dale (2010: 1) believes that the Green Movement's chances of overcoming the state repression strongly "depend on [if] the fledgling movement receives support from abroad . . . In the case of other recent 'colour' (aka 'velvet' or 'soft') revolutions such as Ukraine's Orange Revolution and Lebanon's Cedar Revolution, action by the United States and its allies was critical in ensuring open elections." But despite this relatively common confidence in policy solutions within academia, a well-informed tailored response is yet to be implemented, and many European governments remain unable to consistently and harmoniously regulate the cross-border trade of dual-purpose ICTs inside their borders. This creates, as Tucker (2012: 333) argues, "safe havens where [technologies] might be used for harmful purposes."

What is unique about the Green Movement is its capability to mobilise en masse and unite not only the local dissidents, but also the Iranian diaspora worldwide, whose contributions to the reformist camp had previously remained minimal due to physical isolation. Mostly limited to an undersized elite including veterans of the previous regime (Seattle Times 2009), political activism was far from a common notion among expatriate Iranians until the aftermath of the 2009 presidential election. Posch (2010: 46) assesses that "the [2009] elections politicised apolitical layers of Iran's society in and outside Iran." Pointing at a series

of street protests held by Iranian New Yorkers in support of the Green Movement, Golkar (2011: 56) considers the widespread use of ICTs as the main reason for the successful establishment of a historically absent bridge between local and expatriate dissidents, explaining that "many [local web] users have been able to mobilise Iranians living abroad and bring them to the streets using organisational methods via the Internet." Burns and Eltham (2009: 302) also acknowledge expatriate Iranian communities as an integral cog in the development of the events succeeding the contested elections, highlighting the expatriates' keen utilisation of digital technologies in their protest activities. In their view, the viral dissemination of the audio-visual evidence of the regime's deployment of disproportionately aggressive methods to defuse an essentially peaceful civil rights movement best reflects the role of the Iranian diaspora in framing the "Revolutionary Guard and Basij violence against the street protestors as coordinated destruction—concerted repressive political violence."

Expatriate Iranian cyber-activists and their allies worldwide have been instrumental in the development of various anti-filtering technologies since 2009 (Global Mail 2012). Having observed increasingly successful utilisation of foreign ICTs by cyber-activists in defiance of its sophisticated online censorship system, the regime has routinely charged dozens of local netizens with maintaining 'illegitimate foreign contacts' (BBC 2013). Clark (2011: 32) argues that the only way the regime could have justified its efforts to destroy the Green Movement inside the country would have been to somehow establish its "association with Iranian diaspora around the world," a relatively large number of whom are forced into exile to avoid prosecution, and thus known to be in favour of a fundamental regime change.

The evident reliance of the ruling elite and cyber-activists in Iran on foreign-sourced ICTs raises several questions with regards to the functionality and capability of Iran's National Innovation System, a thorough analysis of which follows in the next chapter.

Chapter ii: Online Technologies, Human Choices and the On-going E-struggle in Iran: Social Shaping of Technology Meets National Innovation System

The interplay between innovation and social change in repressive states remains a largely underexplored area of STS. The second chapter will explain the theoretical undercurrents of this research, by attempting an analysis of the dynamics and patterns of innovation within post-2009 Iran's online political realm.

About a decade after the Iranian regime's first official implementation of online censorship technologies, over ten million websites (Deibert 2008) remain unreachable from inside the country today. Iran has turned into the biggest prison (Luehrmann 2007) for bloggers and journalists in the world. The first question which arises here is how exactly the Islamic Republic has developed one of the most sophisticated internet censorship systems in the world.

STS as a New Mainstream Paradigm: Human Agency, Artefact Trajectory and the Complex Nature of Innovation

Given the reciprocal nature of innovations (Valovirta 2012), socio-technical systems are the conceptual cornerstone of the STS school of thought (Ellinas et al. 2014). Amongst the many theories proposed since the early days of STS, SST is a highly prominent one which gives compelling weight to sociological variables, at the same time as recognising the certain characteristics with which individual technologies may be associated (Basden et al. 2011; Magaouda 2014). If a functional NIS requires that the three essential spheres of authority, business and academia, then innovation processes can best be explained through an interdisciplinary approach. Therefore, as with any other form of serious inductive research, it is a balanced focus on the interaction of the social and the technical that can promise to decode innovation processes and their surrounding patterns – a conveniently overlooked notion by the determinism advocates, which largely consist of business entrepreneurs, online security experts and computing engineers (e.g. Gratton 2010).

What gives mainstream STS its current authority (Jasanoff 2003) is its fundamental focus on the principle of mutual shaping. Historically, techno-society researchers (e.g. Negroponte et al. 1997) have emerged from a deterministic background regardless of their respective discipline. When it comes to new innovations, the end user has often surprised design engineers in terms of 'legitimate' use. Therefore, "social learning [is] crucial to how generic ICT capabilities are applied and used in particular settings" (Williams et al. 2000: ii). STS, on the other hand, draws the attention to the sociological significance of taking into account constructivist notions such as "uncertainty, peer reviewing and the settling of scientific controversies" (Bauer 2009: 5) – although it must be acknowledged (Wesselink and Hoppe 2010) that the peer reviewing practice alone cannot always be a convincing determinant of academic validity.

The sociotechnical environment in its current form is stranded in a contradictory state whereby both business enterprises and governmental institutions are often discouraged or even unable to interact efficiently due to profound ideological differences. Both these economic forces are just as often left with no choice but to adapt themselves to the risks of a highly politically charged climate. This paradox calls for the introduction of a new, future-

oriented analytical framework within emerging economies in order to help revive what Borup et al. (2006: 287) refer to as the "promissory properties of innovation networks."

This interpretation of STS does not build merely on the technical capacities of ICTs, but instead on the social and cultural factors and values under which individual technologies have been innovated. Sociologically, it translates into putting a firm emphasis on the case-by-case, content-based observation of relevant new media accounts, asking "whether there is evidence that people are collectively finding ways to appropriate, adapt and actively shape the use of digital technologies to take [a more purposeful] control of time" (Wajcman 2008: 67).

Despite what it might seem, not only this approach to STS is not disruptive to constructivism, but it can be highly beneficial to finding new links between various seemingly disconnected studies across disciplines. In search of a definitive solution, Kelly-Garrett (2006: 203) finds a need for the development of an innovative system which can help locate all "existing and new work" within a comprehensive framework. This research builds on Lynch and Cole's (2005: 272) conception of "accountable science and technology" to further examine this relatively young strand of STS.

Technological Determinism, Social Bias and the Humanitarian Significance of the Constructivist Response: An IS Perspective

Innovation processes are occasionally viewed by some (e.g. Barney 1991; Shapiro 2010) as technology-driven – a theoretical angle rejected by most IS analysts (Fritsch 2011; Niklasson 2013). The constructivist school of thought promotes a dynamic approach to innovation. From an SST perspective, new technological artefacts are all but fortuitous (Nambiar and Kennedy 2012; Teixeira and Werther 2013). This analysis method not only prevents biased or opportunist commentators from taking undeserved credit for functional, people-driven advancements, but also helps reinforce any future promises which those advancements may possibly hold.

The global STS debate is currently polarised between two mainstream and equally forceful models: the one that suggests innovation systems can perfectly function under an economically sound, but not necessarily a democratically inspired, regime dismissing the significance of the co-evolutionary dynamics between society and technology, and the one calling for an outright dismantlement and restructuration of the undemocratic systems, striving to shift the general focus of the scholarly research towards the historically less promising (Franzese 2014; Smith and Lee 2015) theories of political science. There is, however, a conveniently overlooked alternative, which seeks to put forward policy-making as an alleviator of the social concerns and values as defined by most constructivism scholars – a finely conceptualised proposal argued by Woodhouse et al. (2002: 298), who view the main role of regulatory practices to be the global promotion of "a more democratic, environmentally sustainable, socially just, or otherwise preferable civilisation." From the perspective of the EU, the politically most powerful (Jørgensen 2006) decision-making institution in terms of foreign policy, bringing closer the diplomatic efforts and hi-tech innovations is vitally important to the worldwide promotion of democracy in the 21st century. On that note, S&T and foreign policies, as Stein (2002: 463) asserts, "can be mutually reinforcing in the quest for a better global future," helping transform the dynamics of power in repressive countries like Iran.

Based on this outlook, the main focus of the international control systems should not be on the technical artefacts or the 'legal' bindings associated with them in certain repressive states, but instead on independent assessments of the possible modes in which those technologies can be adapted and used by the potential end-users worldwide. Any approach other than the above, as Woodhouse and Patton (2004: 4) argue, will inevitably lead to the dead-end that is either technological neutrality or determinism, which they describe as "folk theories that attempt to...explain [the human-technology] interaction in black-and-white terms, attributing agency either entirely to people or entirely to technology."

The validity of this view has been recognised by the even less constructivist STS researchers such as Lynch and Cole (2005), who propose a hybrid of social and technical as an ideal theoretical framework for scrutinising the sophisticated nature of human-technology interactions.

The very foundation of this branch of constructivism was laid over two decades ago by Haraway (1994: 59), who pioneered a thought school which fundamentally ruled out the neutral and deterministic doctrines, setting the main emphasis on the highly dynamic ideas of reconfiguring "what counts as knowledge" and reconstructing "the generative forces of embodiment."

Rooted theoretically in techno-feminism, Haraway's "Cyborg Manifesto" seems to have formed the basis of a reformist movement which over a decade later put the concept of participatory technology on the map together with the other mainstream theories of social innovation. Among the most progressive of these theories developed to date is SST in which, according to Tedre et al. (2006: 128), "the abstract and the concrete interweave", and cliché terms such as performativity, "efficiency and predictability" are positively eliminated from STS.

Cyber-Activism, Modern Social Movements and Advanced ICTs' Patterns of Creation and Use in Repressive Contexts

If we consider the technical innovations to be a reciprocal process of socio-technical dynamics, then a functional NIS simply cannot be planned or designed on a top-down basis. Otherwise, any progress resulting from the system will only stand to serve the politically powerful strata of the society. But a temporary shortfall may not necessarily mean a permanent failure, as ICT innovations can at any stage be highly responsive to creative user inputs regardless of the scope of their intended or perceived functions (Gounari and Grollios 2010; Valkenburg 2012).

In repressive states, the industries have no choice but to become a subordinate to the desires of the dominant political elites. While it might seem pragmatic to assume that all the social researchers are by default empathetic toward philanthropic ends, their work is in reality sometimes influenced by economic agendas, including those dictated by the government. This idea points out (Frickel et al. 2009: 446) to an increasing need for pioneering, agenda-setting academic studies, even if they may suggest outright "conflicts with the interests of elites."

The typical users of activism-oriented ICTs across geopolitical borders have repeatedly shown a keen tendency to favour social, cultural and environmental justice over technocratic and economic gains, or as Smith (2005: 109) views it, to support an alternative which aims to

"identify scope for further improvements, or even adapt the technology to uses unanticipated by the original designers" – a phenomenon markedly demonstrated by the Iranian cyber-activists after the June 2009 turmoil. This points to an emergent cyber-activist system of innovation comprising a network of local and expatriate political dissidents, which as evidence shows is considerably less concentrated and resourceful yet equally knowledge-oriented, as compared to the regime's online censorship apparatus. For the purpose of conceptual clarity, this thesis defines a system as a "group or combination of interrelated, interdependent or interacting elements that form a collective entity" (Rouse 2003: 33) often characterised by change (Padoch and Sunderland 2014), which follows a set of rules and values in its persistent pursuit of an ultimate cause.

One of the main reasons behind the scholarly community's relative inability to explain the sociological roots of cyber-activism is the common yet overly simplistic analysis (Qiu et al. 2009) of the information divide phenomenon based on the user's economic background. That is why there is a crucial requirement (Selwyn 2003: 101) for a "systematic and objective understanding of individuals' non-use of information technology", particularly within undemocratic environments. Some prominent feminist scholars (e.g. Wajcman 2007; 2008; 2009; 2013) have laid the foundation for this through their fruitful attempts to theorise the human-technology relationship with regards to socially vulnerable user groups.

This casual reduction of compound concepts such as computer and network literacy to static concepts such as user skills merely infecting (Gunduz 2010: 45) "elderly people, some categories of housewives, illiterates and the unemployed," stems typically from a deterministic school of thought which subconsciously undermines the all-important sociological undercurrents behind the issue under scrutiny.

The utopian view on rapid, scalable technological advancements as typically championed by repressive governments, which essentially forms the above rhetoric behind the digital divide phenomenon, tend to build chiefly on Habermas's notion of scientisation of politics (Wajcman 2013: 349), according to which "political problems are seen as technical ones [...whereby] the expert directs the politician." But contrary to this narrative, not only the consumers of a given ICT do not passively receive it as an inflexible, static tool, but instead they actively seek to "alter the meanings and deployment of technologies" in direct accordance to their very social aspirations and needs. Further contributing the argument at hand is the work of Huyer and Mitter (2003: 7), who deem the "communication, critical thinking and problem solving skills" to be far superior to the industrial output volumes and sheer technocratic ambitions in terms of the national economy.

The key to decoding this puzzle is to approach the matter from a carefully examined perspective, and one that has the capacity as well as the aim to explain the nature and mechanisms of the interplay between structure and agency in the field of STS beyond technocracy and in a more contextual sense than is conventionally pursued – a fact thoroughly reflected in the evidence extracted from the study of NIS structure and functionality in individual countries. If else, many future research opportunities could be wasted on methodologies which fail to acknowledge the basic fact that even the most ancient fabrics of literacy (i.e. reading and writing) are influenced (Livingstone 2003: 4) broadly by "power and authority to access, interpret and produce printed texts." Such a delicate goal will need inevitably to acknowledge that the internet, despite some media propaganda, has not fundamentally transformed the trajectory of social activism, but instead has developed it into an "available toolkit of action forms" (Van Laer and Van Aelst 2009: 234). Given this, ICTs

ought to be viewed as an influential factor, but not a revolutionary force, when it comes to social protest. The electronically mediated means of communication do not by default enable mass protestors to succeed, or as Yzer and Southwell (2008: 11) put it, "radically break social barriers to have...previously unimaginable conversations." Instead, they remain to be a mutual, renegotiated (Flanagin et al. 2010) product of the interaction between the social and the technical which tend, in nearly all repressive contexts, to be solely shaped by the ruling political elite.

National Innovation System: Theory and Practice

Many Innovation System (IS) theories and theorists—such as Social Systems of Innovation (Amable et al. 1997), National Business Systems (Whitley 1993), Technological Systems (Carlsson and Stankiewicz 1991), Regional Systems of Innovation (Cooke 1992; Maskell and Malmberg 1997), Sectoral Systems of Innovation (Malerba and Breschi 1997)—have tried to explain the structure and functionality of a country's knowledge production system at various points in history, often with the aim of improving their homeland's economic status through identifying and addressing the barriers against growth. Among these models, NIS is perhaps the most wholesome and comprehensive concept developed to date. The origins of the NIS theory seem to go back to the late 19th century, when List (1841) first introduced a theoretical framework he referred to as the National System of Political Economy (NSPE) to help Germany catch up with the then much more industrial England. Preparing the ground for a range of policies focused on the production and application of new technologies, his advocacy was "one of the main factors in Germany overtaking Britain in the latter half of the nineteenth century . . . [and] the foundation for the superior skills and higher productivity of the German labour force in many industries" (Freeman 1995: 6). List was the first scholar to recognise the "interdependence of the import of foreign technology and domestic technical development . . . [and the idea that] nations should not only acquire the achievements of other more advanced nations, they should increase them by their own efforts." He was the first scholar in the history of the discipline to bring together the two notions of education and infrastructure building together in a bid to create a robust domestic production system, and to rule out Smith's (1776) cosmopolitan approach which considered cross-border knowledge trade as a consistently beneficial procedure for all the parties involved.

The first scholar to speak distinctively of NIS was Freeman (1982), whose work built directly on List's National System of Production (NIP). Originated at Sussex University's Science and Technology Policy Research Unit (SPRU), Freeman's theory was different from that of List in the sense that it focused on the "importance of an active role for government in promoting technological infrastructure . . . [and the circumstances under which] free trade will promote economic development" (Johnson et al. 2004: 2). This was closely followed by Lundvall's (1985) introduction of Innovation Systems (IS) at Aalborg University's Innovation, Knowledge and Economic Dynamics Research Group (IKE), which built largely on the same concepts and literature. Since the mid-1980's, Freeman and Lundvall worked separately and together to improve the concept and turn it into a coherent model. While the NIS model is deeply rooted in Western culture and is specifically developed to address the innovation issues in open political systems, Johnson et al. (2004: 2) note that "some of the most important elements going into the combined concept actually came from the literature on development issues in the third world," where lack of economic development remains a top concern for local Innovation Studies scholars. But NIS is simply not designed to be applied to semi- or un-democratic states, which calls for a set of alterations to help tailor the theory for such case studies.

Unlike Freeman, Lundvall et al. (2002: 215) suggest that the IS theory as we know it today "was not based upon any direct inspiration from List [and that it] was only after the concept had become generally accepted that Christopher Freeman . . . went back and brought forward List as the intellectual ancestor." Instead, they identify the concept with Linder (1961). Conversely, Lundvall's work is thought to have been greatly inspired by that of the MIT-based Von Hippel (1976). But apart from minor disagreements on the origination the NIS model, scholars remain largely in agreement about its core, which has been unfairly criticised on a few occasions as well. Patel and Pavitt (1998: 3) define NIS as the study of the "institutions involved in the generation, commercialisation and diffusion of new and better products, processes and services (i.e. technical change), and of the incentive structures and competencies in these institutions that influence the rate and direction of such change." Putting a techno-political spin on the model in question, Carlsson (2006: 58) describes it as "a set of distinct institutions which jointly and individually contribute to the development and diffusion of new technologies and which provides the framework within which governments form and implement policies to influence the innovation process. As such it is a system of interconnected institutions to create, store and transfer the knowledge, skills and artifacts, which define new technologies." With regards to the founding fathers of the theory, however, one cannot ignore a difference in the core focus of their work. As Niosi et al. (1993: 208) observe, "technological flows and technology development interaction among firms appeared to [Lundvall] much more frequent within national boundaries than across borders [while] Christopher Freeman put the accent on social and political institutions that accompany technical innovations . . . not simply those in direct charge of R&D activities."

A turning point in the development of the NIS theory into more of a flexible, internationally usable concept was perhaps the work of Carlsson (2006: 58), who argued that "depending on the purpose of the inquiry, the most useful definition of innovation systems might not coincide with national borders." This was particularly salient for developing, undemocratic countries, where dependency on foreign sources of technological innovations remained a serious issue. Previously, Fagerberg (1994, cited by Patel and Pavitt 1998: 3) had identified "two essential components of . . . knowledge generating activities: education and training in all countries, and R&D in the industrially advanced countries," which not only shows he believed in the flexibility of the NIS model, but also underlines the extent to which he appreciated education as an influential factor in developing a nation's innovation possibilities. An inter-disciplinary approach supported later on by many other innovation scholars (Doloreux 2002; Dutton 1996; Ruttan 1997) puts the emphasis on educational, social and political processes and their control over the trajectory of technological artifacts, as opposed to leaning towards the economic factors and how the research and development budget is managed. This breakthrough in the history of the study of innovation systems helped open the way for future extension of the theory to undemocratic states. This brings us right back to Freeman's (2002: 193) emphasis that NIS can be traced back to List, who too saw "that industry should be linked to the formal institutions of science and of education . . . [adding that] List's book on *The National System of Political Economy* might just as well have been entitled *The National System of Innovation*, since he anticipated many of the concerns of this contemporary literature."

The main argument often put forward by the critics of the NIS model, as Etzkowitz and Leydesdorff (2000: 110) report, is that "academic technology transfer mechanisms may create unnecessary transaction costs by encapsulating knowledge in patents that might otherwise flow freely to industry." But the above scholars rule out this criticism by emphasising that knowledge would not be "efficiently transferred to the industry without a

series of mechanisms for identifying and enhancing the applicability of research findings"—a concise argument that truly captures the core essence of what the theory represents. But what even the most devoted adherents of Freeman and Lundvall seem to overlook is that openness is prerequisite to a functional NIS. Freeman and Lundvall's original model is best applied to North-Western European countries, where lack of democracy is hardly a tangible issue. Features of a democratic system, therefore, have been considered as given in the formulation of the concept. The identified gap in this otherwise robust theory prevents it from being directly applicable to repressive countries, where the nationwide innovation processes are often distorted by ruling elites' ideological or militaristic approach to the generation and diffusion of scientific knowledge—in this case, IRGC's clout over the Iranian mass economy. While the dysfunctions of an undemocratic state's NIS may seem to be a positive incident to some radical activists in the West, I argue otherwise. A repressive regime's monopolistic approach to technological innovations creates division within a country's NIS, which will in return weaken the domestic pro-democracy forces, who are denied their fair share of research and development budget. Under the circumstances, the problem will not merely be a lack of financial resources, but rather a pattern of allocation dictated by senior IRGC security officials, who are increasingly resorting to ICTs in their bid to defuse opposition. This secretive approach also restricts the regime's chances of recruiting appropriately-skilled candidates, which it has traditionally addressed through resorting to European innovations. This, in turn, points to a weakness in Western policy, which currently remains imperfect in terms of regulating intercontinental technology trade ethics. Deprived from accessing or contributing to any scalable in-house stream of technological contributions, the cyber-activists are meanwhile forced to rely solely on the limited attention they occasionally receive from Western democracies. This division, along with the religiously-motivated gender inequality that exists in most repressive countries (Kanwar 2009), has made Iran's NIS a dysfunctional one.

Another noteworthy limitation of the NIS theory, in its traditional form, is its lack of elaboration on cross-border influences on the innovation processes in a given country. NIS was originally designed with the relatively small, stable and secular Northern European (e.g. Nordic) states in mind: countries where the government officials are democratically elected and religious or militaristic goals do not determine the trajectory of technological artifacts (Christoffersen et al. 2010). In such circumstances, the expatriate factors become much less relevant, for several combined reasons. For one, these countries remain largely independent and at the forefront of exporting hi-tech, telecommunications innovations (World Economic Forum 2012). Further the rate of emigration of highly-skilled forces from these countries remains extremely low due to the high quality of life, with Northern European citizens' occasional choice to live outside their country rarely being politically-motivated or permanent (Huffington Post 2012). It is yet rarer that people from these nations dedicate their lives to careers of radical political activism (Ervasti et al. 2008). This is simply due to the already high rates of social tolerance and inclusiveness along with the highly democratic nature of the Northern European political regimes—eliminating the need for organised resistance. The above factors result in a classic, functional NIS maintained by all members of the society regardless of their political tendency, location or gender.

This research was first inspired by Mackenzie and Wajcman's (1985) *Social Shaping of Technology*. SST argues that technological changes are not the result of an inner technical logic and that human choices, whether made consciously or unconsciously, can actively influence the direction of innovation trajectories. In their thorough analysis of the socio-economic processes influencing technological innovations, Williams and Edge (1996: 866)

suggest that SST "has been forced to go beyond simplistic forms of social determinism which, like technological determinism, see technology as reflecting a single rationality—for example an economic imperative, or the political imperative of a ruling elite." The theory stands distinctly apart from Social Construction of Technology (Bijker et al. 1987; Pinch 2008; Pinch and Bijker 1986), also known as SCOT, which represents a more socially deterministic approach in comparison. Based on SST, it is reasonable to argue that the trajectory of online innovations in Iran is neither arbitrary nor accidental, but rather largely shaped by the long-term objectives and strategies of the Islamic Republic, which controls the key means of Research and Development (R&D).

The main hypothesis of this dissertation has been founded on a number of IS theories and concepts such as the National System of Political Economy (List 1841), NIS (Freeman 1987), the Learning Economy (Lundvall 1995) and Diffusion of Innovation (Rogers 1983), and on the research of scholars such as Nelson, Edquist and Sclove among others. While the NIS theory originally refers to the flow of information among people, enterprises and institutions and how they interact, there is no generally accepted view as to what the structure and functionality of a country's IS should be like. Iran's NIS is unique, and this thesis has employed Freeman's conception of NIS only as a baseline to develop a specific model for Iran.

NIS Functionality: From Nordica's Ordinary Choice to the Developing World's Ultimate Dream

Despite various conceptual shortcomings (Bugliarello 2011; Cimoli and Porcile 2010), the NIS theory remains to be the social constructivists', as well as many other STS scholars' (e.g. Pinto and Santos-Pereira 2013; Qi 2011), preferable choice of theory for studying the emerging economies.

The NIS theory has not been sufficiently critiqued by STS scholars researching the developed economies (Kwon 2010). The main body of the critical NIS literature produced by non-Western academics tends to stem from isolated, crisis-driven studies of political flashpoints rather than from concrete, original social research based on inductive methods. A great example of this is Ikejiaku's (2014) publication on the international laws of commerce, in which he accuses unfoundedly the entire industrialised world of conspiracy to "legitimise colonialism, acts of exploitation . . . [and striving merely] to protect, project and promote the interest of the [West]."

The geographical divide between Eastern and Western oriented STS literatures raises the paradigm-altering question of whether the IS approach to techno-activist research is a conductive or an inductive one in nature. While many experts (e.g. Asheim and Gertler 2005; Fagerberg et al. 2009) in the highly industrialised democracies of Northern Europe traditionally have found NIS to be a socio-technical fit for their respective nations, various attempts to apply the concept to non-Western countries have failed to prove fruitful due to intricate contextual clashes and incompatibilities across national borders.

Today, local and regional circumstances have been largely respected by most EU regulations, where "strongest linkages are to Nordic countries, especially to Finland and Sweden" (Danielyan and Wittbom 2009: 30) – homes to some of the largest ICT innovators in the world. If we recognise the true organisational complexity in being "a free market economy and at the same time a Nordic welfare state" (ibid: 30), then no emerging economy can

remotely compete with its top European (i.e. Finnish or Swedish) counterparts in terms of NIS capability and functionality.

Based on the above, the practical applicability of the NIS theory as an economic driving force stands profoundly different in the West from that in a developing country like Iran, where all major R&D decisions and plans are made as part of an ideological system with economically unjustified development priorities. This calls for a critical cross-examination of major previous scholarly attempts at the universalisation of NIS.

NIS in Emerging Economies: Theoretical Gaps in the Literature

As the main body of NIS became more focused on already highly industrialised European countries immediately after its instigation, the concept has become less relevant to the underdeveloped economies of the third world. Although relatively limited, part of the Eastern literature (e.g. Arocena et al. 2014) attempting at the development of the NIS theory steps indeed in the right direction.

NIS has evolved and expanded considerably over the recent decades. If there is one key element that makes the theory conceptually superior to its counterparts with regards to social research, it will have to be its cohesive ability to locate nationwide innovation practices at the "heart of discussion on upgrading and growth" (Chaminade and Vang 2008: 2).

The rapidly changing chain of events in the emerging economies has somehow left the NIS theory inefficient in terms of universal application. A prime instance of this theoretical shortfall is the emergence of affluent, yet technologically underdeveloped firms in the South-East of Asia, whose relatively extended global presence is rooted predominantly in what S.H. Chen (2004: 341) calls the rise of "leapfrogging competition", where the institutionally favoured companies in the developing countries form a habit to invest generously in latest successful Western innovations, without having fully decoded the previous generation(s) of the technology involved. Although often highly rich in terms of physical assets, these firms are almost consistently behind their Western counterparts with regards to the prolific production of internationally transferrable scientific knowledge.

In STS, indigenisness encompasses "coherent systems of . . . explanation that . . . can often offer better accounts of local phenomena than those theorised by Universalist science" (Bebbington 2001: 7293). This stands distinctly apart from endogeneity, which refers (Jackson 2012) to that "which comes from within a given society, and to the specific characteristics, values, ideas, knowledge, institutions and practices that pertain within a society." Thus, while many NISs in the emerging economies can be considered somehow indigenous due to their instinctive adaptation of the 'natural' scientific knowledge, seldom any of them are truly endogenous in sociotechnical terms.

Indigenous technology might be simply an outcome of various 'catch-up' techniques and practices such as reverse engineering, social appropriating or even outright off-setting. In the case of either modes of Iran's NIS, foreign purchases almost consistently take precedence to innovation, especially when it comes to ICT advancements. Largely due to structural issues caused by contextual circumstances (e.g. IRGC's belligerent foreign policies), this finding has been reflected substantially in the answers given by the experts interviewed throughout the project. The notion of endogeneity has never been a priority or even a real possibility in the

telecommunications industry in Iran, as the country's main innovation actors are too poorly managed and coordinated to function as a unified, dynamic system of optimal standards.

The import-oriented characteristics of NIS in Iran link directly to the democratic degree (i.e. gender neutrality) of the construction of its major industrial actors. Subsequently, the relative uniqueness of the Iranian NIS model lies within its characteristically charged suspension between adaptation and imitation, which has ultimately led the country to a state of technical unsustainability. Iran's vulnerable place as a relatively passive consumer in the worldwide knowledge-production picture can be compared in many ways against the historically prominent example of the World Health Organisation's struggle with the implementation a new health management information system in Uganda in 1993, where Gladwin et al. (2003:) highlight the West's lack of attention to "organisational context when . . . attempting to understand the causes of information management problems . . . in [underdeveloped] countries." The technologically dependant nature of all such states translates into import-oriented development strategies, with excessive financial expenditure on foreign expertise seen as a remedy for the country's systematic failure on the indigenous innovation front. This capital-driven trend has had serious implications for the NIS theory.

Apart from making fundamental contributions to STS throughout its history of existence, the NIS theory in its current form tends (Lyasnikov et al. 2014; Watkins et al. 2014) to have one more remarkable flaw when it comes to the emerging economies, which is its relative inability to explain the inevitable, yet varying degrees of a state's technological reliance on foreign, more technologically advanced sources of innovation. Although many scholars have recognised NIS to be the most suitable conceptual framework to employ in the modern studies of sociotechnical policy with a primarily Western focus (Ernst 2002: 4), it is crucial to note that the NIS in the developing countries tends to operate on a hybrid and sometimes even a bifurcated basis, where "very limited sharing and pooling of resources occurs within the country," and where an assembly culture formulates the nation's "main vehicle of learning and capability formation" (ibid: 4).

A slight form of this systematic malfunction is reflected in the state of NIS in South Korea, Taiwan and Singapore, whose core approach to innovation has traditionally been an economic-driven one. Unlike in the industrialised democracies, the authorities in these countries seem to have built their NIS on a foundation of financial investments, where the main focus of the major universities, institutions and enterprises is on a "well-developed system of management of technological diffusion" (Mathews 1999: 1), as opposed to a bottom-up, indigenous and knowledge-based structure.

The general structure of the so-called catch-up economies may have roots partly in their universities insistence on direct application of the Triple Helix model as the prevalent model for their nationwide innovation programmes. While TH is known to be a perfectly functional model in politically open contexts, a great majority of the emerging economies (e.g. South Korea) seem to suffer from a "lack of collaborative networking" (Shapiro et al. 2010: 3), preventing the framework in question from successfully mimicking the levels of functionality at work in the decentralised Western European systems.

Among these states, the case of Singapore is a perfect evidence of how a country's NIS can economically advance, but not necessarily make any progress towards the top of the global innovation tree, resulting in very little levels of investment (Wong 2003: 191) in "indigenous companies and small and medium-sized firms."

A similar argument applies to South Korea, which is further proof as to why simply attempting to duplicate the various measures taken by a functional NIS without taking into account the various unique characteristics of the destination country is an essentially flawed model. Therefore, although commonly viewed as one of the most industrialised nations in its geographical region, "the lack of basic technology [has become] the weak point of Korea's NIS" (Yim 2006: 157).

This pantographic policy employed by some developing states in the Far East may have helped them achieve more financial gains to date than they would have otherwise. But with them having increasingly turned into a "global factory" (Ernst 2006: 3) as a result of their excessive focus on global sales, they have been in effect reduced to competent adaptors of imported expertise at best. But the mere scale of manufacturing output cannot accurately determine the social sustainability of a given NIS. For instance, although Japan was the main provider (Borras 1997; Branstetter 2001; Ernst and Guerrieri 1998) of civilian technologies used actively by the US and Canadian military forces toward the end of the 20th century, the NIS in those countries was never deemed by mainstream STS scholars as dysfunctional or inefficient. On the other hand Japan, a once highly applauded producer and exporter of high-tech electronic goods, is no longer a leader in the global ICT community, nor does it seem capable of posing any serious threats to the West in terms of indigenous ground-breaking innovations.

Even in scarce cases where non-industrialised countries have tried to challenge the knowledge gap at the academic level, their major universities' focus has remained largely on learning and not innovating (Assmann and Stiller 2014; Cappelli et al. 2014), and on catching up instead of leading. The South Asian governments, which often bank on the management and diffusion techniques as opposed to developing their own R&D solutions, usually have their eyes set on profitability and hence have neglected those enterprises interested in endogenous innovations (Intarakumnerd et al. 2002) as a general rule.

Reversing the emerging economies' unoriginal approach to ICTs requires no less than an ideological transformation across their inner circles of political power, in terms of willingness to reprioritise the society's genuine needs through investing in home-grown research projects, as well as a redefinition of their innovation ambitions within their academic means. From an STS perspective, such systems have two major issues to overcome (Wong 1999) if they are ever to pursue the suggested route: being culturally and politically detached from the leading Western research centres, and not having an immediate access to the lucrative Western markets.

NIS Variations, Indigenous Technology and Cross-Border Dependency: What Makes Innovations Socially Sustainable?

Since its dawn on the emerging economies, asset development, but not technological endogeneity, seems to have become the key indication of functionality in NIS. Instead, this research proposes that cross-border reliance needs to become a key determinant of economic success in the developing world. Therefore, the present application of NIS in the developing countries is not only inadequate, but also confusedly justified in terms of theoretical depth. Conversely, to suggest that profit planning is an unorthodox business management tactic would be equally redundant. The intellectual dilemma between morality and lucrativeness can, to some extent, obscure the boundaries between ethical and unethical practice.

Politically-closed regimes, such as the communist party in China, are yet another commonly ignored reason why the innovation systems are contemporarily viewed through a technocratic lens, turning into a cog within the state's security-driven, outsourced approach to technological innovations. When tested under such binary circumstances, mainstream NIS theory in its existing formula proves largely to remain restricted to democratic contexts.

One must never forget the profound impact of the socio-political factors on the on-going status of a nation's NIS. China, one of the fastest growing economies in the world, owes its economic stability chiefly to its communist regime's fundamental reforms within the political realm, which subsequently transformed the country into the "biggest production hub" (Altenburg et al. 2008: 333) for the US as well as for the rest of the OECD states in Europe and elsewhere. However, the Chinese owe too much of their economic success to "adopting and using ideas and products developed elsewhere" (Chang and Shih 2005: 155), placing their NIS under the same category as that of their Iranian counterpart in terms of self-efficacy and output originality.

Iran's NIS: An Empirical Analysis of a Bifurcated Structure

There is little evidence of any domestic efforts and investments within Iran aimed specifically at self-sufficiency with regards to cyber policing. While government-sponsored experts and engineers have been having a hard time keeping up with the pace of advances in anti-censorship techniques, there is substantial evidence that the regime's strategy to outsource the job has proven more successful. Western telecommunications conglomerates have occasionally contributed to the suppression of online political activists in Iran over the past decade. Some of these companies have sold Iran's security officials complex internet censorship technologies, while others have equipped them with tools useful in screening and locating individual mobile phones, as well as with machinery designed for jamming satellite TV and radio signals broadcasted from the West.

Before a thorough analysis of the socio-technical dynamics of political change in Iran is possible, it is necessary to map out and explain the country's National Innovations System (NIS). Described by Lundvall (1992: 2), an NIS explicates "the elements and relationships which interact in the production, diffusion and use of new, and economically useful, knowledge . . . [which] are either located within or rooted inside the borders of a nation state." Due to Iran's complex socio-technical dynamics, this study will focus less on Nelson's conception of an NIS, which tends to put the main emphasis on national research and development policies, and more on Lundvall's broader notion, which pays a particular attention to learning and education. In the following analysis of the Iranian NIS, the three core elements of higher education, governmental institutions, and private enterprises will be considered, and their interplay with one another will be closely examined.

As was seen in the case of Iran's nuclear ambitions and its production of long-range missiles, most of its internal innovations were developed secretly by a handful of well-protected scientists based at specialist academic and military research centres—specifically at the Ministry of Defence's Malek Ashtar University and IRGC's Imam Hossein University. Generously funded by top security officials, both institutions are universities of military science and technology offering only a limited number of undergraduate and postgraduate programmes to a small number of students (mostly qualified officers) filtered through an intense selection process. Many of the rest of the Iranian regime's various politically motivated technological innovations take place at IRGC's Baqiyatallah Medical Sciences

University and at Sharif University of Technology, one of the country's most prestigious science and engineering universities, which runs an extensive nuclear technology programme. Although the latter institution is public and therefore not restricted to the IRGC—and indeed mostly free from its control—nonetheless, it is technically where the most valuable military/dual-use innovations happen, due to its high standards of research and quality of equipment and laboratories. All the above universities are located in Tehran. The following figure shows the Iranian regime's nationwide system of military innovations:

Iranian Regime and the Technologies of Mass Destruction

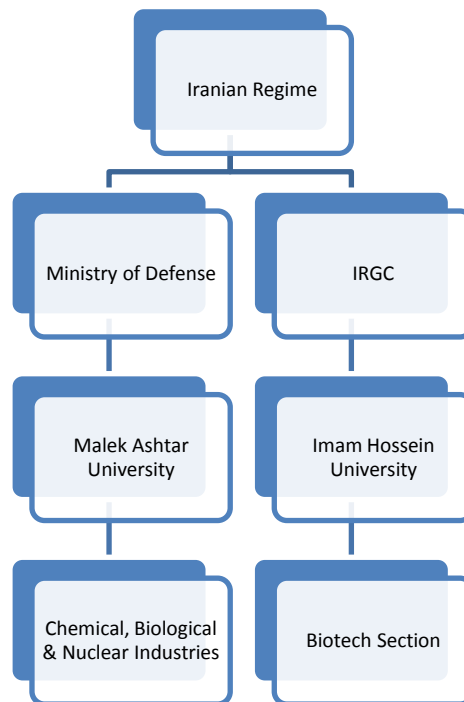


Figure 1 (Spiegel Online 2003)

Patterson and Smith (2005) name five of Iran's major universities as centres where hacking innovations may be happening: Sharif University of Technology, the University of Tehran, Amirkabir University of Technology, Isfahan University of Technology and the University of Isfahan. This list has been composed by the above authors largely based on a content analysis of the academic staffs' online profile pages and/or personal blogs, as opposed to concrete evidence substantiating that they are in fact engaging in such activities. Their observation, therefore, can at best only confirm the above universities' capacity to train professional hackers and to develop hacking software, rather than proving that they are undoubtedly doing so. Politically motivated hacking attacks are often conducted as a result of complex psychological processes. They are not normally deployed merely to show off technical ability. In one instance, Patterson and Smith point to Dr. Shahram Bakhtiari of Sharif University of Technology's personal webpage having a presentation titled "hacking techniques" posted on it. Yet they state that they could not open the file due to a broken URL. Even if the webpage in question was indeed a hacking tutorial, it could simply be a routine security lesson required by the module of study, and would not directly reflect Dr. Bakhtiari's or his students' political ideology.

So, without clear confirmation that Iranian universities function as centres of security-oriented innovations, how then does the Iranian regime upgrade, operate and maintain its online censorship infrastructure? Green Voice of Freedom (2010) reports that IRGC has set up seemingly private front companies in order to seek and hire professional hackers to teach hacking methods to officers in Iran's Cyber Army—an organisation claimed by the regime to be the second largest of its kind in the world. Operating secretly and in parallel with the country's formal higher education institutions run by the Ministry of Higher Education, "these companies [are] responsible for instructing hackers and accomplishing Iranian Cyber Army projects. [They] are also involved in importing military technology for the Iranian armed forces," the website states. Sabeti (2011) quotes IRGC Commander Brigadier Ali Fazli, deputy head of Basij, as saying on 13 March 2011 in an interview with Mehrnews Agency that "the cyber section of the Basij . . . includes professional hackers from different branches of the Basij among university lecturers, students, students of religious seminaries and women." He also quotes him on the close co-operation of the cyber branch of Basij with IRGC as explaining that "the reason for the major breakthroughs of the Revolutionary Guards has been their reliance on the services of the Basij experts." This is against the country's laws on cyber-space passed in the Iranian Parliament (Majlis) on 31 January 2011, according to which destruction, manipulation, theft or interception of another's private electronic data or interception of private conversations transmitted on the internet or through any other wired or wireless form of telecommunication is deemed to be a criminal offense and punishable with imprisonment and/or fines (Majlis 2011). Yet the regulations do not clarify the lawmakers' standpoint on hacking activities aimed at internal opposition or a foreign state, and even if they did, it would be naive to expect parallel extra-judicial apparatuses backed by the Supreme Leader to feel bound by them.

The IRGC was formed by Ayatollah Khomeini shortly after the Islamic revolution in 1979, as a loyal parallel to the regular army forces, many of whom were conscripted soldiers inherited from the previous regime and hence not necessarily very dedicated to the Islamic Republic's policies. The IRGC was a ministry within the government and under the President's direct command for a long time, acting largely as an extra defence mechanism helping to establish border security and assisting the country's other armed forces against foreign threats (such as during the Iran-Iraq war), but it was later on separated as an extra-judicial entity placed under the Supreme Leader's control. Today, with about 125,000 members, this unelected body has grown to be one of the most powerful institutions of the Iranian regime, engaging in a wide range of activities from dominating import/export markets to leading and strategising the regime's nuclear programmes, from media censorship to arresting, detaining and interrogating the political activists.

The following figure illustrates the general structure of the IRGC:

The Hierarchy of the Iranian Regime

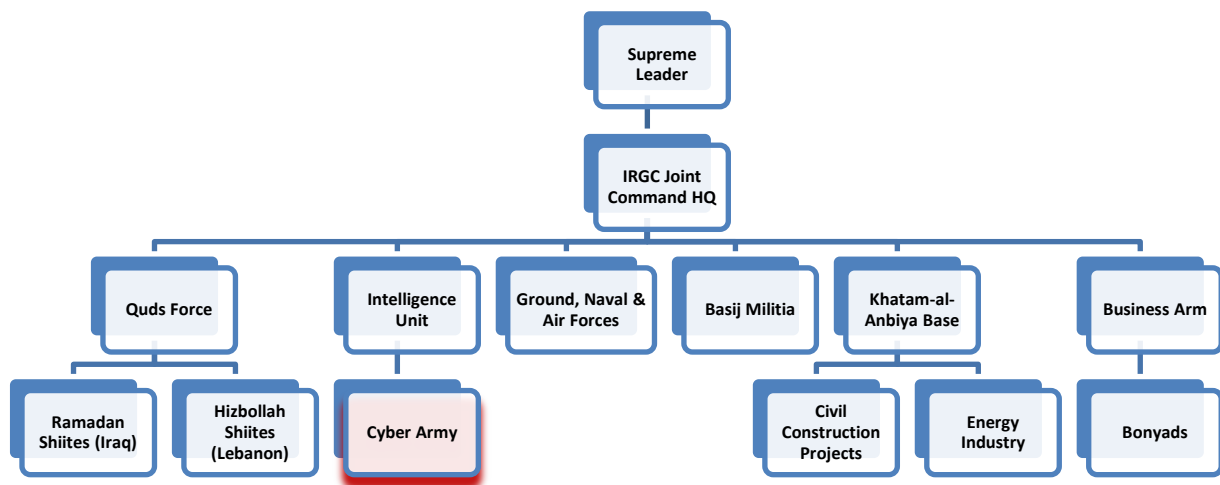


Figure 2 (Higgins 2010)

While Iran's Cyber Army may indeed be large (the exact population serving is unknown), the number of truly expert hackers it employs cannot be nearly sufficient to develop, implement, operate and maintain the world's most sophisticated internet censorship apparatus (International Business Times 2012). Therefore, the majority of online censorship technologies currently in use in Iran are imported from Western, mainly European, ICT companies via IRGC's front companies. With Iran's NIS failing to meet the ruling elite's technological needs, the IRGC manages to acquire almost any sensitive telecommunications technology via proxy from anywhere in the West. Published by an anonymous UK-based Persian blogger, the following picture shows an example of the satellite signal jamming machines installed on Tehran's Milad Tower, the tallest building in the country:

A Satellite Signal Jamming Machine Installed by the Iranian Authorities



Figure 3 (Spy Blog 2009)

According to this photograph, the device is manufactured locally by Saber Co., a subsidiary of the IRGC. But the technology behind these machines has most probably been imported. Further, in a Health Ministry report confirming the health dangers of long-term human exposure to signals from these devices, a government official's repeated denial (and in some cases criticism) of the devices in question could be yet another indication that it is the IRGC, not the Ministry of TCI, that has the ultimate control over the regime's censorship initiatives. The September 2009 takeover of the Telecommunication Company of Iran, the TCI Ministry's biggest contractor and the Iranian equivalent of BT, by the Mobin Trust Consortium (aka Etemad-e-Mobin—another IRGC sub-company) following Ahmadinejad's decision to privatise parts of the country's telecommunications industry is proof of the neo-conservatives' keen desire to gain sole charge of the country's national and international gates of the flow of digital information—a dream which has largely come true at this point in time.

Although a great deal of concern has been expressed by international regulatory bodies over Iran's alleged pursuit of WMDs, neither the UN nor the EU provide much evidence regarding the Islamic Republic's use of imported ICTs to silence pro-democracy dissent. According to Deibert and Rohozinsky (2010: 3), despite IRGC authorities continuously denying ownership of TCI, they seem to have an increasingly easier time analysing the country's online access points. "In countries where the lines between public and private authorities are often blurred, and/or organised crime and authority mingle in the dark underworlds, such informal requests and pressures can be particularly effective, opaque and nearly impossible to bring to public account" (ibid: 3).

Confirming the IRGC's vast use of imported technology to address its censorship needs, Karlekar and Cook (2009: 100) have found substantial evidence that some Western telecommunications technology companies actively aid the regime's "censorship and surveillance practices, [providing] equipment that is crucial to carrying out such tasks and at times [turning] over the personal data of users leading to their arrest." These companies compromise their ethical values despite sufficient knowledge of the Islamic Republic's illiberal nature. Some companies have denied these allegations by emphasising Iran's seemingly top rated cyber strength and its ownership of one of the most sophisticated online censorship systems in the world. The only way to scientifically examine and disprove such an argument would be via a thorough analysis of the country's NIS.

Iran is a repressive state where protecting national security against foreign threats is often reason enough for the regime to avoid transparency. It isolates its innovation centres and restricts access to a narrow number of elite scientists. In such circumstances, where any type of technological innovations potentially useful in the defence industry are tagged as confidential, neither competition nor collaboration is viable—yet both are cornerstones of a healthy, functional NIS. Sun et al. (2010: 2) suggest that the "dynamics of the NIS are becoming an important source for national competitiveness." These dynamics largely consist of the way various elements of a country's NIS interact with and complement one another. A defective innovations cycle, as is the one currently in place in Iran, would result in a weak NIS, which will subsequently seek to fill its gaps by resorting to foreign expertise.

Realising the national importance of innovation, Japan, a country heavily damaged during the Second World War, managed to recover itself and become one of the world's strongest economies in less than half a century. Freeman (1995: 12) contrasts Japan's highly integrated NIS with that of Soviet Union, where there was a "huge commitment . . . to military and space applications with little direct or indirect spin-off to the civil economy . . . Three-

quarters of the massive Soviet R&D resources [went] into defence and space research," not leaving much space for civil innovations. Freeman counts three main reasons for the failure of the Soviet Union's NIS in the civil innovation sector: "The Soviet system grew up on the basis of separate research institutes within the academic system . . . [and] the links between all these different institutions and enterprise-level R&D remained rather weak . . . Moreover, there were quite strong negative incentives in the Soviet system retarding innovation at enterprise level, such as the need to meet quantitative planned production targets . . . Finally, the user producer linkages which were so important in most other industrial countries were very weak or almost non-existent in some areas in the Soviet Union" (ibid). Japan importantly detached its NIS from an isolated, uncompetitive and secretive military industry, and designed a carefully regulated innovation system along with policies that ensured transparency and competitiveness at all times. This model is currently far from being employed in Iran. Abbasi and Hajihoseini (2004) explain that "the Iranian innovation policy system lacks an overall vision, integration and policy coherence." Mani (2004: 22) notes a number of technology support institutions and policy instruments in Iran, almost all of which function in isolation, leading to the emergence of a fractured, dysfunctional innovation system. "Given the very highly concentrated nature of the manufacturing sector and the continued domination of public sector enterprises, [encouraging innovative efforts in manufacturing enterprises] is more likely to remain a policy objective for the future," he argues.

Similarly, Ghazinoori (2004a: 11) reveals that about sixty-five per cent of all the Iran's major research and development centres are military-run and hence located in the capital city Tehran. He finds that "there are many research activities being conducted in the defence industries which have achieved tremendous results in the fields of manufacturing ammunition for the military forces . . . However, there [is] no appropriate relationship between the defence research section and non-military areas." His results complement those of a United Nations (2005) report on the ownership status of most of Iran's large and medium-sized companies. This report holds low representation of the scholars in work in the private (civil) research centres responsible for the overall failure of the country's ICT innovations. "In 1996, the total number of researchers, research assistants and technicians amounted to 68,385 persons, of whom 82 per cent were employed in public sector institutes and 18 per cent in private sector research centres," the UN report discloses. Salami (2008: 6) also asserts that Iran's industrial competitiveness is in urgent need of innovation-friendly policies led by academia and industry. According to him, "innovation possibilities cannot be taken as a given. Innovation is a capability that has to be developed. It can be said that despite the move towards a knowledge-based economy, innovation has not yet become a strategic goal of policymaking in Iran."

This top-down approach—primarily designed to give priority to the demands of a secluded elite—stands right against Lundvall's original model of an NIS based on inter-sectoral flow of knowledge and collaboration. This, in turn, raises the question of how legitimate it is for Western telecommunications technology companies to help rectify the technological deficit of a system that remains dysfunctional primarily due to its undemocratic nature. Ghazinoori (2004b) explains that in countries like Iran, where the regime plays a key role across a variety of business territories, and thus ultimately determines the technological artifacts and the market dynamics, the NIS has little choice but to fail. He suggests that the Iranian government should refrain from dominating the country's economy and instead support the development of bottom-up innovations. "In countries like Iran the market demand is formed upon observing foreign products rather than on the basis of domestic technological power, as

a result [of which] domestic technology can hardly meet the demand, and importing foreign technology is inevitable . . . research activities are just decorative and have no relation to the country's real needs . . . [and] no technology growth can be expected," the author claims. The following figure demonstrates the contrasts between the Iranian NIS with that of a typical Western, industrial country.

Iran's NIS is top-down and mainly funded by oil revenues—one reason why the first round of the Western sanctions was directly aimed at Iran's energy exports:

Oil Income and the Iranian NIS



Figure 4 (Ghazinoori 2004b)

On the other hand, a successful NIS, as theorised by Lundvall, would function based on minimal governmental intervention, and maximal independent research, largely reflecting market demand, rather than being held hostage to official dictation:

Lundvall's Cycle of Innovation

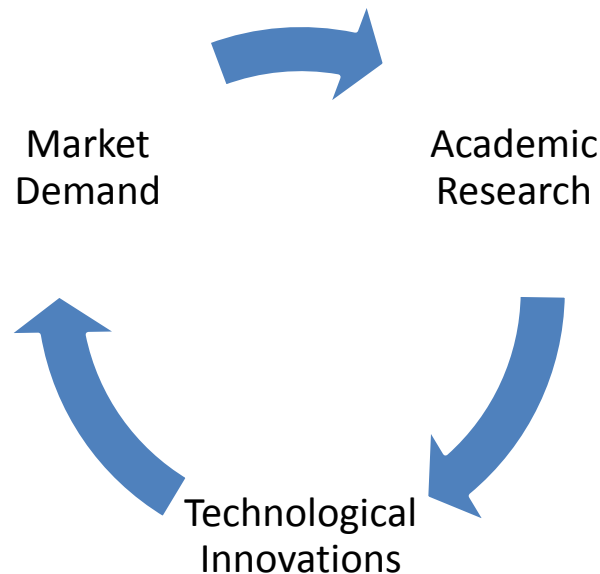


Figure 5 (ibid)

Iran's currently linear and one-dimensional model of national innovation, as seen above, is its source of economic deterioration and a reason behind its self-insufficiency. Ghazinoori (2004a: 10) considers the geographical centralisation of Iran's 'prestigious' technological universities as one of the main consequences of the Iranian regime's attempt to divert the innovation processes in its favour. "Due to the lack of practical facilities and inadequate practical experiences among the professors, the graduates of the engineering fields have poor innovation and fail to use their skills for the higher level R&D activities," the author argues.

The Iranian NIS, in other words, is not reliant on market demand or academic expertise, but instead on orders from the political elite. The United Nations report (2005) primarily demonstrates that Iran's innovation failure is one caused by weak and partially non-existent relationships between the key components of its NIS.

While the report shows a relatively high expenditure on higher education compared to total government expenditure (20.4 per cent), it also exposes the country's metaphorical Achilles' heel: Iran's technology-based exports accounted for only two per cent of total exports. "Iran's expenditure on R&D activities as a proportion of GNP is only 0.5 per cent. In order to transform its economy into a technology-based one, Iran needs to increase its R&D expenditure substantially," the report reveals. Yet even the regime's high investment in academia does not necessarily entail that funds are distributed evenly or fairly or that they are allocated based on civil priorities and national interests. Implicit in Ghazinoori's (2004a: 11) analysis is the perception that the problem results from of a lack of proper funding dedicated to appropriate parts of the educational system: "Eighty per cent of the country's researchers are working in the universities, while only 20 per cent of the research budget is allocated to [them]. Academic research in Iran is usually conducted without considering the needs of the market" (ibid: 11). Furthermore, Maleki et al. (2005) found that the two weakest functions within Iran's NIS are knowledge development and market formation. While the latter element is not entirely relevant to the core focus of this study, the following table shows a list of the negative factors currently influencing the former function in Iran:

Inhibitions and Barriers to the Iranian NIS

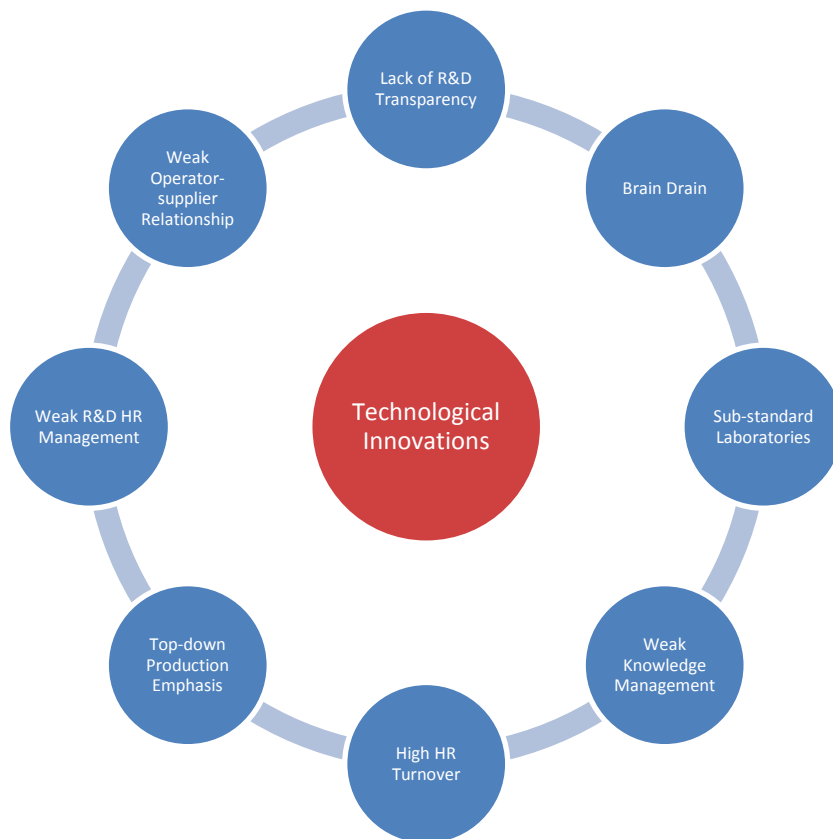


Figure 6 (Maleki et al. 2005)

Rezazadeh-Mehrizi and Pakneiat (2008: 88) observe an overly large presence of international hardware and software suppliers in Iran's mobile and wireless industry, which happens to be monopolised by the IRGC-run Bonyade Mostazafan. They state that domestic industries in Iran need to be developed in an evolutionary fashion, further elaborating that "what [is] missing here [is] the starting point for this evolution process that could hardly be found in domestic dimensions." Looking back at the United Nations report (2005), it is evident that results from Iran's knowledge system hardly percolate into the country's production system. The report concludes that "the enterprises only undertake production, but do not perform innovation activities. While such a strategy was sufficient to cater to an import-substitution economy, it is not a dynamic capability for sustainable development" and further determines that even Iran's large, state-owned manufacturing enterprises rely on technology imports in order to meet their needs. This thesis adheres to Etzkowitz and Leydesdorff's (2000) Triple Helix Model (THM)—a well-developed IS concept that puts the main emphasis on academia, while encouraging intense collaboration among all three main elements of an NIS in fulfilling their roles, which the developers of THM see as often interchangeable.

The THM, as Etzkowitz et al. (2007: 14) describe it, represents "overlapping, yet relatively independent, institutional spheres," and is a flexible model which emerging economies should embed into their long-term development plans:

Triple Helix Model

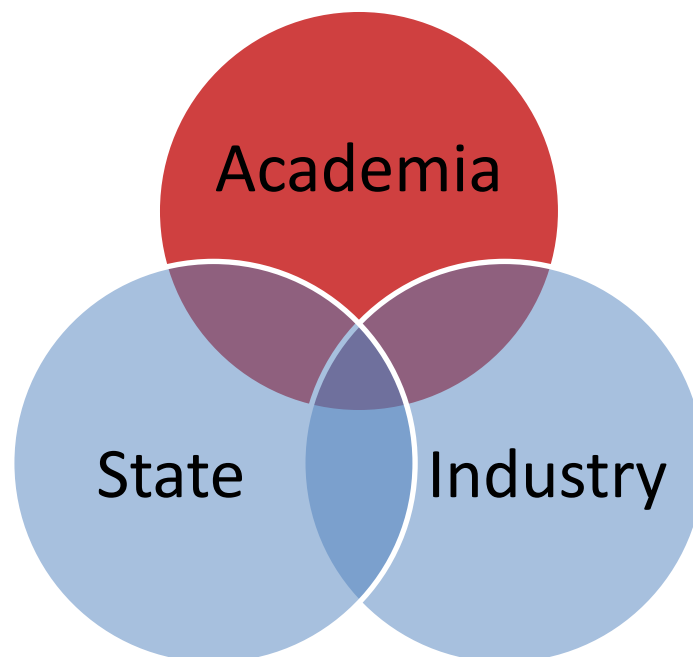


Figure 7 (Etzkowitz and Leydesdorff 2000)

Differing in essence from THM, the following graph illustrates the theoretical dynamics of the Iranian NIS in place today:

Regime's Innovation System in Iran

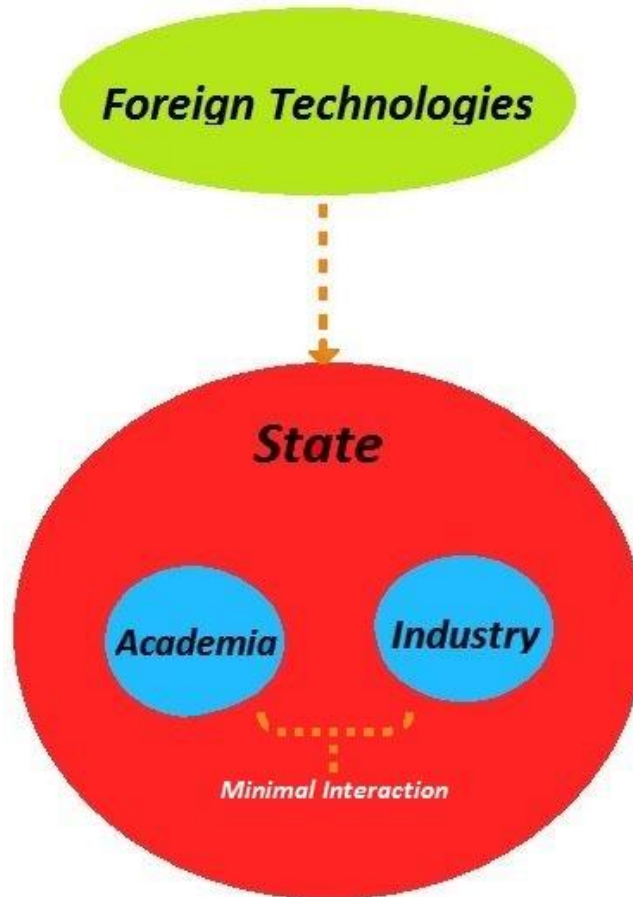


Figure 8

Unlike in THM, Iran's NIS is characterised by heavy influence from state-run, security-oriented organisations and survives mainly through foreign technology imports at nearly all levels. What distinguishes the two models even further is the gradual disconnection of the country's scalable enterprises from academia, as these are increasingly merged into the IRGC's nationwide economic empire. The reliance of the Iranian NIS on foreign technologies, therefore, is a direct outcome of its distortion-induced failure.

NIS Dysfunction in Iran and the Country's Inevitable Reliance on Foreign ICTs

As the Revolutionary Guards rapidly expand their domain in business, a significant and often adversarial separation remains between academia, enterprises and institutions. Under such conditions, the country's overall innovation output can only be minimal at best, making imported ICTs a very attractive option. Vaughn (2005: 9) criticises Microsoft, Cisco, and Oracle for encouraging the militarisation of Iran's economy in their trade with the Iranian regime, and argues that most Western ICT companies are prepared, on some level, to suspend codes of corporate social responsibility in return for guarantees of substantial economic profit. He accuses these companies of "trying to bend every which way they can to help anyone with a deep pocket" (ibid). Figliola et al. (2011: 11) confirm that the Nokia-Siemens Network (NSN) sold online censorship equipment to the Iranian government in 2008,

elaborating that "the monitoring centre, installed into the MCIT gateway, was part of a larger contract with Iran that included mobile phone network technology."

Pleading innocence, Western telecommunications technologies firms have typically justified their business engagement with repressive states by highlighting their legal obligation to provide certain 'counter-crime' features to their 'elite' clients all over the world, as part of standard service packages. There has been very little research done on the functionality of Iran's NIS, and the main body of literature available publicly has been produced inside the country, where university-based research is heavily monitored, making it difficult to rely on. Iran's case is a blatant example of a bifurcated NIS, where military-oriented innovations remain a priority in comparison to the civil ones.

The relationship between recent online innovations and social developments in repressive countries is best explained via the Ukraine's Orange Revolution—the world's first and arguably most ICT-driven political uprising. Internet and democracy experts, such as Goldstein (2007), have argued that digital technologies played a substantial role in the expansion of Ukraine's Orange Revolution (OR). Other cybernetics scholars, like Lysenko and Desouza (2010), have gone so far as to call OR a 'technology-assisted' resistance, which this study finds rather technologically deterministic. A contextual analysis of the Orange Revolution will follow in chapter six.

In order to be able to construct an analysable framework relevant to innovation processes at work in present Iran, the methodological design of this research stays almost entirely focused on the period after 2008 and 2009, which witnessed the country's economic system go through major, costly structural transformations (Tehran Times 2010). Following Mahmoud Ahmadinejad's contested election as President in June 2009, Iran saw a major boost in the Islamic Revolutionary Guards Corps' (IRGC) role in the country's economic and political affairs, in part due to Ahmadinejad's status as an ex-IRGC official (Cordesman and Seitz 2009). In Ahmadinejad, the IRGC found a 'friendly' figure in charge of the government following sixteen years of fruitless (Al-Monitor 2013) reformist efforts. Today, the IRGC fully controls about 70 per cent (Institute for Middle East Studies 2011) of Iranian industries, extending its influence from 'security-related' industries to a variety of profitable fields ranging from the manufacturing and importing of fast moving consumer goods (FMCGs) to banking and medical and educational services (Iran Watch 2013). Such activities on the part of Ahmadinejad's neo-conservative government were aided by the presence of a mostly conformist parliament, elected in 2008 with historically low citizen turnout (Farhi 2008), resulting in the formation of what is arguably one of the country's most hard-line legislatures since the 1979 Islamic revolution.

Even in a Western democracy, there are normally several conflicts of interest between higher education and military institutions, suggesting that the direction of research and development budget allocation at country level will be heavily influenced by the values of sponsoring organisations. In other words, any institution that funds a scientific study remains essentially in control of the socio-political rhetoric that the outcome of that project is likely to convey. All research is conducted for specific reasons, one of which is often the desire to create profound 'change'—an inherently subjective concept. However, one man's scientific progress can only equal the violation of another's rights. As seen below, militaries exist primarily to 'protect.' They are regimented, biased and conformist. Universities, on the other hand, are mostly liberal and flexible in nature and encourage innovation.

The following table demonstrates the core differences between military and academia in terms of construction and values as well as their relationship to the wider society:

Organisational Values: Military vs. Academia

	Military	Academia
Organisation	<ul style="list-style-type: none"> - Strong Structure - Clear Relationships among Components 	<ul style="list-style-type: none"> - Weak Structure - Fuzzy Relationships among Components
Values and Beliefs	<ul style="list-style-type: none"> - Duty, Honour and Country - Service - Bravery - Obedience - Intolerant of Ambiguity 	<ul style="list-style-type: none"> - Freedom of Inquiry - Education - Intellect - Questioning - Tolerant of Ambiguity
Relation to Wider Society	<ul style="list-style-type: none"> - Service Ethics - Quite Removed - Conservative 	<ul style="list-style-type: none"> - Iconoclastic - Somewhat Removed - Liberal

Table 1 (Herrmann and Douglas 1996)

Taking these characteristics into account will help make better sense of nationwide innovation processes in Iran, where the intelligence unit of the IRGC and Basij militia along with senior security officials within the Ministry of Defence has woven a tightly-knit network of support within the country's universities, in a bid to prevent 'counter-revolutionary' scientific ends from being pursued in academia. A prominent result of this effort is the arrest, conviction and imprisonment Dr. Omid Kokabi, an Iranian nuclear physicist (NPR 2011), for 'co-operating with hostile governments.' It can be argued that the ruling elite in Iran have a multi-layered apparatus in place in order to ensure that the generation and diffusion of scientific knowledge in academia occurs without surprises. This is particularly crucial in non-military universities and research centres, where the students might not necessarily be ideologically 'fit' to serve the long-term interests of the Islamic Republic.

The Iranian regime's ideological approach to new technologies can be seen as an example of what Neriya-Ben Shahar and Lev-On (2011: 876) call Religious Social Shaping of Technology (RSST), where "ideology attempts to protect and strengthen it, the liminal spaces between ideology and practice." This model focuses on religious groups who see their traditional values threatened as a result of freshly emerging technological practices and whose position stands sharply opposed to that of the proponents of openness and civil liberties, who often employ the same technologies in order to foster and promote democratic activities. While there is hardly a shortage of deterministic theories in the field of STS, evidence (Feenberg 2006) suggests that the correlation between internet and democracy can best be explained through a constructivist approach, most prominently Mackenzie and Wajcman's (1985) Social Shaping of Technology. Arguing that cause-and-effect approaches such as technological determinism are "at best an oversimplification," and that "changing technology will always be only one factor amongst many others," Mackenzie and Wajcman (1999: 7) define the politics of technology as "any systematic attempt to ensure that the surprises are indeed good ones." Despite their generally negative approach to new technologies, the Ayatollahs in Iran have made every possible effort to utilise ICTs as a force to help them maintain control over the country's political discourse. But they have also calculatingly dismissed certain technologies. The best example of this would be the Ministry

of Communications and Information Technology's initiative (ARS Technica 2012) in 2011 to replace the regular internet connection with a 'halal' alternative—an essentially parallel Local Area Network (LAN) isolated from the rest of the world. This project was widely mocked by the cyber-activists worldwide and referred to as the 'filternet.' The plans were soon cancelled by senior security officials who denied it altogether.

As the Ayatollahs too must have realised, there are many legitimate reasons why so-called cleansing of the internet would not work in Iran, despite allegedly 'successful' implementation in other repressive countries such as China, North Korea and Saudi Arabia. Jillian York (2012a), director for international freedom of expression at the Electronic Frontier Foundation in San Francisco, described three main causes for the Iranian authorities' inevitable back-down from the plan, only one of which was purely technological—the incapacity of Iran's cyber-police as compared to China's. She reasoned that Iran's banks and international businesses, along with many other commercial firms within the governmental and private sectors, would suffer mightily from the internet cut-off, and that "such a move [would] be damaging . . . to the country's economy, unsustainable without global connectivity." She also pointed out an often ignored yet important sociological fact, which particularly distinguishes Iran from North Korea: "Iranians have developed a taste for the global internet . . . through the use of proxies and VPNs . . . Any attempt to block the social networks Iranians have become accustomed to would surely result in an uproar." The bottom line is that the main purpose for the censorship system Iranian political leaders have implemented today is not—as claimed—to block pornography, but instead to tackle politically motivated online activism. As York shrewdly observed, "if Iran were to insist on censoring obscenity, it could take different measures . . . Instead, the government seeks to tear its citizens away not only from the global internet, but from communicating with their families and friends abroad." Technical choices like these turn ICTs into a powerful oppressive force in repressive countries—one with prioritisable effects.

Perhaps the biggest differentiator between China and Iran in terms of how they approach online censorship lies in their economic structure and functionality as opposed to a systematic pursuit of endogenous innovation. Although there is a significant variance of opinion among scholars about the exact influence of online technologies on modern social movements in the emerging economies, King et al. (2013: 15) highlight the consistent "relevance of technological innovations on the longevity of authoritarian regimes worldwide." This thesis argues that the degree to which a repressive regime chooses to block online channels of communication depends primarily on its ability to afford developing and implementing the often much more expensive alternatives. From a financial perspective, it is always much more expensive for an autocratic government to purposefully manage, rather than fully disrupt, the flow of online information. This simply means that despite the common perception, a dynamic stream of online communications does not necessarily need to be damaging to the legitimacy and political clout of a repressive regime, if that regime has the resources to effectively monitor and process the information on a mass scale. Therefore, as China "devolves the bulk of censorship responsibility to internet content providers, [its] regime maintains large economies of scale in the face of new technologies" (King et al. 2013: 15).

In spite of their occasional propaganda, the Chinese authorities' willingness to control, and not as much block, online content is manifested in their record-high investment (\$6.5b in 2015) in high-tech start-up companies. The critical truth here for the Chinese political leaders is that their two-decade-long trail of vast economic growth would not sustain in the long run,

if they were to pull the plug on the online sphere altogether – a strategy favoured strongly by the North Korean generals. As Wired (2015) assesses, "the [communist] party is worriedly seeking new sources of good jobs [and] technology fits the bill."

Unlike in Iran, we are witnessing in China an NIS that is relatively effective in shifting from imitation to indigenous growth and development. This is not, however, least because of the dynamism of China's economy or the expansion of technology-related business in that country. It is, rather, due to the emergence of a young middle class of entrepreneurs oriented to business, as compared to the general inclination to foster bottom-up political opposition as is the case in Iran.

Also, the bottom-up opposition in China is tightly controlled when it appears to move toward organising a mass protest against the state. The Chinese regime seems to fight direct opposition by a combination of severe clampdowns, at the same time as adopting populist policies aimed at challenging state corruption. This makes China an increasingly affluent and hard-shelled dictatorship, which as King et al. (2013: 15) argue, "is probably being watched closely by autocrats from around the world."

Western scholars (e.g. Posner 1961: 323) have widely acknowledged the notion that "differences in the rate and nature of innovation in different countries" can determine the state of their economic growth. Souitaris (1999: 295-6) proposes based on his robust comparison of national innovation in Iran and Greece that the "portfolio of important determinants of innovation is wider for countries with competitive market structure and support for entrepreneurship than for centralised economies." The portfolio of evidence gathered by this thesis in relation with the dynamics of technological innovation in Iran highlights markedly the applied significance of what Souitaris calls the "attitude of management" toward other main variables within an innovation system such as R&D, skills and competition. He concludes his investigation by stating that "In Iran, large firms were all public and highly inefficient. Therefore, the small firms were more innovative despite their primitive management systems."

On the other hand in China, although large firms usually "attract more bureaucratic intervention and hence may be less efficient than small firms" (Zou and Adams 2008: 1149), they are at the same time known (Kinkel et al. 2015: 7) to be "more active in building up value added activities in foreign countries than small and medium-sized enterprises." In their search for the 'truth' on how technology affects the economic growth of a given national economy, Soofi et al. (2013: 57) divide major market-based economies of the world into two distinct categories of efficiency-driven (i.e. Middle East, Asia-Pacific) and innovation-driven (i.e. Western Europe, North America)", with the lead differentiator between the two being endogeneity. By conducting a comparative examination of NIS in Iran and China, this research has attempted to further explore the former category, in hope of advancing the state of scholarly knowledge on the determinants of ICT (e.g. online) innovation across less democratic political contexts.

The Social Shaping of Technology is at work not only in spheres controlled by the regime—pro-democracy cyber-activists have also been busy utilising and adapting newly available ICTs as means to their ends. The dissent-friendly capacity of ICTs was already discovered nearly a decade ago by Lievrouw (2004: 11), who observed that "new media modalities . . . made formerly obscure activist subcultures more accessible and open to people who are seeking diverse political opinions or new avenues for political participation." In fact, there

have been many scholarly attempts (Earl and Kimport 2011; Kelly-Garrett 2006; Van De Donk et al. 2004) over the past decade to establish a robust, coherent relationship between concepts of social activism and telecommunications technologies. Very few of these studies, however, distinctly argue that the internet's political power does not lie in its 'inherent trajectory,' but rather in the way it has been utilised by already active, well-connected groups of likeminded political activists across geographical borders. Recognising the reciprocal, co-evolutionary nature of human-technology interaction is crucial to understanding the complexity of the socio-technical mechanisms of political change in repressive countries.

This research can be seen as a constructivist response to either extreme of deterministic discourse. In addition to recognising ideas such as Kalathil and Boas's (2003) concepts of Civil Society Organisations (CSOs), e-propaganda and international sphere, it also occasionally acknowledges the inbuilt characteristics of individual technologies. The need for such an approach is reflected in the concept of dual-use ICTs, which as demonstrated below, are potent telecommunications technologies with varying degrees of applicability in both civil and military industries.

Authoritarian vs. Civilian Technology Advantage

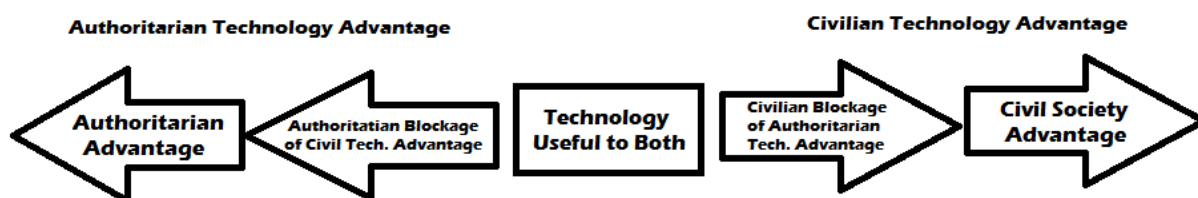


Figure 9 (Joyce 2011)

Bearing the above in mind, the following graph illustrates the structure of Iran's current NIS, in relation with the country's on-going power struggle, and builds theoretically upon existing interdisciplinary literature:

Foreign Technologies, IRGC and the Online Power Struggle in Iran

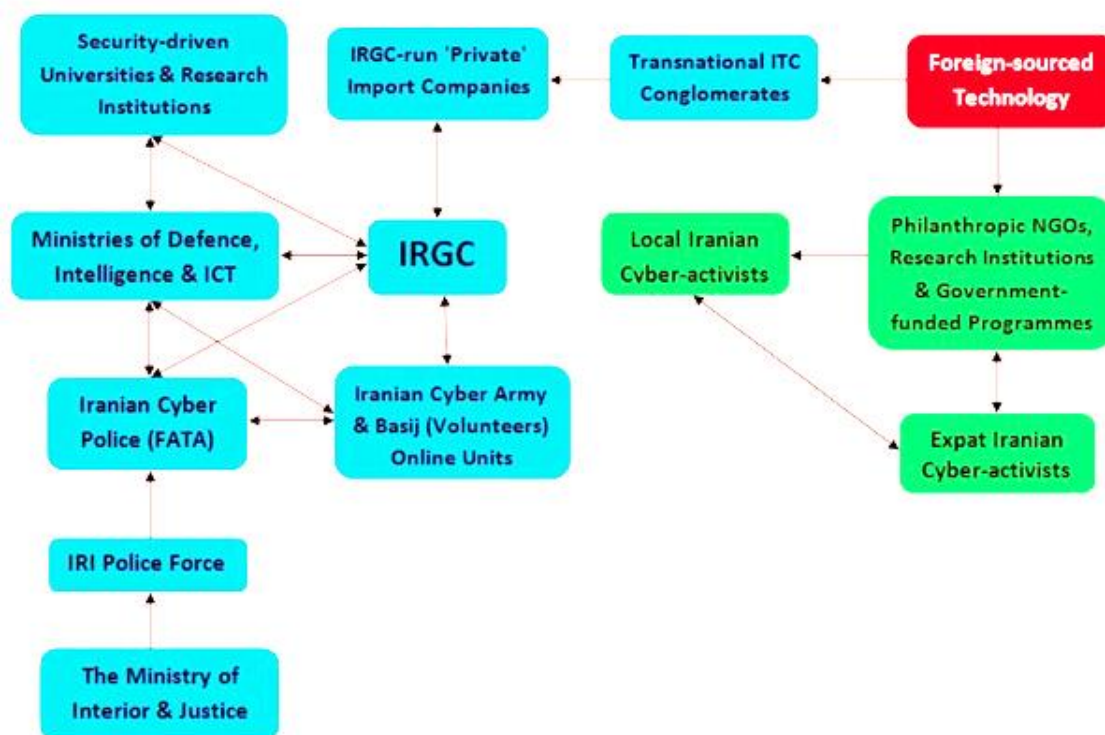


Figure 10

Understanding the origins of telecommunications technologies employed by the cyber-activists and the regime requires a thorough analysis of the country's NIS. Careful scrutiny of this under-theorised structure is particularly important as the dynamics of innovation in Iran are fundamentally different from those in Western democracies, where NIS theory was originally developed. Unless we comprehend a given nation's mechanisms of innovation and how they function, we can neither competently explain the local contribution of ICTs to political developments nor effectively address policy gaps in ways that would promote democracy or weaken repression.

Forty per cent (All Voices 2010) of Iran's economy was reliant on EU companies in January 2010. But very few Western ICT firms have either admitted to any ethical errors on their part for engaging in this trade or even officially responded to accusations raised against them by human rights advocates worldwide. Leberknight et al. (2010: 4) point the finger at a range of well-known firms including Secure Computing, Nokia-Siemens Networks and Allot Communications, arguing for directly culpability as "there are not many commercially available censorship technologies," and that such technology can only be tailored on demand. They divide the available censorship technologies into two main categories of software and hardware, the former suited to filtering content and the latter useful in classifying network traffic and inspecting packet headers and payloads (also known as Deep Packet Inspection). Every repressive government needs its own specific technological features, depending on the scale of resistance it faces, along with its own ideological objectives. Deibert (2008: 331) holds commercial software to account as responsible for most of the online censorship taking place in autocratic countries, suggesting that "these products . . . have been readily employed by censoring states like Tunisia (Secure Computing), Iran (Secure Computing), Myanmar (Fortinet), and Yemen (Websense) to block access to politically-sensitive content." OpenNet Initiative's statistics (2005; 2011b) show that Deibert's insights into online censorship are

likely to be accurate. According to the organisation, the main internet censorship software used in Iran by the Iranian government since the mid-2000s is SmartFilter, which is a commercial content filtering tool developed by Secure Computing, a McAfee sub-company based in San Jose, California. The following statement has been extracted from Secure Computing's official response to accusations of unethical business conduct:

Secure Computing has sold no licenses to any entity in Iran, and any use of our software by an ISP in Iran has been without Secure Computing's consent and is in violation of Secure Computing's End User License Agreement. We have been made aware of ISPs in Iran making illegal and unauthorised attempts to use of our software. Secure Computing is actively taking steps to stop this illegal use of our products . . . Unless authorised by the US Government, Secure Computing Corporation prohibits export and re-export of Secure products, software, services, and technology to Iran.

Given that different autocratic regimes have differing overall goals and financial resources, various categories of such technology have developed over the years and been deployed by different regimes. The following figure demonstrates a range of online censorship techniques popular with repressive regimes, organised based on cost and the main political purposes they are designed to serve:

Internet Censorship Technologies: Cost-effectiveness vs. Accuracy

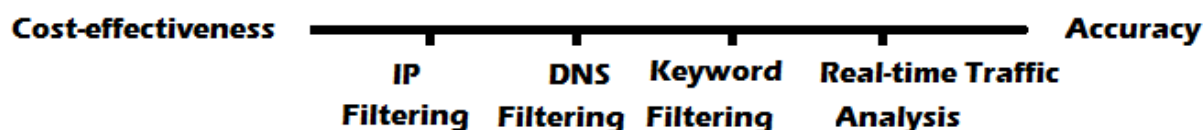


Figure 11 (Wright 2009)

Both SmartFilter and SurfControl belong to the cheapest and hence the least accurate filtering method (IP Filtering), demonstrating that most repressive regimes are content with static, categorical blockage of websites, as opposed to active surveillance of individual users' traffic (routinely practiced in China). In authoritarian countries, the government's primary aim is to display an ability to maintain 'full control.' This precedes any interest in the very difficult and costly job of identifying and arresting anonymous cyber-activists. While many well-known cyber-activists have been subject to prosecution in Iran due to their online activities, there is no concrete evidence that the regime has made any systematic attempts to identify or locate anonymous web surfers based on the nature of their traffic. These relatively cheap and inaccurate filtering methods also result in the permanent blockage of thousands of 'clean' websites. The following snapshot of SmartFilter's URL database taken in 2008 demonstrates how the Secure Computing programmers have incorrectly classified four of the world's most popular social networking services by tagging them as dating websites:

Filtering Software and Database Compilation

URL	Status	Categorization	Reputation
<input type="checkbox"/> http://www.last.fm/	Categorized URL	- Entertainment - Dating/Social Networking - Streaming Media	Neutral
<input type="checkbox"/> http://www.livejournal.co ...	Categorized URL	- Dating/Social Networking - Blogs/Wiki	Neutral
<input type="checkbox"/> http://www.orkut.com/	Categorized URL	- Instant Messaging - Dating/Social Networking - Web Mail - Media Sharing	Neutral
<input type="checkbox"/> http://www.twitter.com/	Categorized URL	- Dating/Social Networking	Neutral

Table 2 (OpenNet Initiative 2011b)

The above example is a simple demonstration of how politically motivated technological choices can go wrong. As the decade-long history of internet censorship has shown, repressive regimes are likely to be more dissatisfied with the popularity of online social networking and its viral effect than they are to be annoyed with readership of foreign news websites or pornographic content. Naturally, social networking platforms are where most online innovation diffusion occurs.

Cyber-Activism: Why Focus on Innovation?

Social movements are by no means a new phenomenon. Historically, the systematic abuse of power by corrupt elites has invariably resulted in the emergence of radical resistance movements aiming to eliminate injustices and establish human rights, either peacefully and through civil disobedience or via means of violence. What is more, political activists have generally benefitted from and almost always relied on technological innovations throughout the global history of revolution. While these innovations vary across a wide range of disciplines, ICTs have intensified power struggles between citizens and states. But communications technology has itself been subject to intense change over the years. It was not until the creation of the internet that scholars began to see a ground-breaking opportunity for transforming the way media can influence political processes. Ever since, untested, techno utopian/dystopian theories relying heavily on assumption have reduced ICTs to either a fully democratic force or a futile oppressor. With regard to communications theory, the internet seems to have caused more scholarly problems than it has solved. There is now a bold theoretical division evident within scholarly literature, while neither side seems to address questions that truly matter to modern pro-democracy movements in repressive states. Even many of those researchers who do come from non-deterministic, constructivist backgrounds have so far focused on Western democracies. Very little in-depth attention has been paid to the application of telecommunications technologies in dictatorships.

ICTs are neither democratic nor repressive in nature. The internet is just another medium of communication, which may or may not be adopted to serve a just or unjust cause. This is not to deny its capacity to influence political discourse, but instead to emphasise the importance of avoiding biased, absolutist approaches in academic research. In order to achieve a realistic, practical model reflecting an accurate correlation between internet and democracy in repressive environments, it is best to consider each case within its own context, while drawing on empirical data from prominent case studies. Khamis et al. (2012: 1) emphasise

the need to consider the roots and functions of "nuanced social, political and communication structures unique to each country, as well as the different roles of their various political actors and the types of online and offline communication strategies they deployed," when studying the interplay between ICTs and democracy. This framework, they argue, "necessitates avoiding the technologically deterministic approach that privileges the tools of social change over the actors that employ them, thus inappropriately elevating social media above face-to-face mass action as agents for bringing about political change."

Since the emergence of the internet, many socio-political 'effects' have been attributed to the medium, yet not all of them have a substantiated evidentiary basis. There has, however, been a positive shift in scholarly literature over the past decade, moving the focus from one-dimensional models such as McLuhan's (1962) Gutenberg Galaxy to Castells' (1996) more dynamic Network Society. As research on the topic rapidly expands, an increasing amount of evidence is stacking up demonstrating the potential of online technologies to contribute to political change, especially in autocratic countries. Yet this includes providing new opportunities to both pro-democracy cyber-activists as well as repressive authorities.

Although it may appear to some quantitative analysts in technical disciplines that the internet has a low penetrative power in emerging economies due to generational, economic and educational issues, there are concealed socio-cultural undercurrents that turn the online sphere into one of the most representational and inclusive communication mediums of our time, even in such contexts. Agarwal et al. (2011: 225) reveal that computational studies of the social media, including Kelly and Etling's (2008) mapping of the Persian blogospheres, have increasingly gained more prominence than empirical accuracy or reflexivity in the recent years. They indicate that such inquiries "predominantly do not study processes involved in collective acts in online environment. They also are mostly based on either link-analysis or content-analysis. They lack insights from social science, such as collective action theories, where issues—shared narratives/repertoires—are important in shaping collective action." The common absence of an STS perspective in recent literature leads to a semi-casual treatment of an otherwise complex multidisciplinary issue. Addressing this gap is one of the main theoretical and methodological aims of this research. This thesis has combined two seemingly unrelated mainstream STS theories (i.e. NIS and SST) in order to reach a dynamic socio-technical model specific to authoritarian states, complementing it with a balanced trio of data collection methods, covering a set of written and oral narratives from activists, scholars and journalists residing inside and outside of Iran.

STS literature also comprises a multitude of techno-dystopian arguments. Pickard (2008: 626) notes that "the democratic theory embodied by [online] political actions is frequently neglected altogether in existing scholarship." Palczewski (2001: 162) asserts that research on the internet has largely dismissed social movement and protest theories, which has led "internet studies [to] replicate both traditional social movement studies' focus on the state and modernists' limited understandings of political participation." The dominant rhetoric in these studies seems to be that ICTs are far too deeply embedded into average citizens' lives to be considered a separate force. The truth is that many of the studies in the field have overlooked the influence of innovation processes on political change, focusing either on developing a new conception of Social Movement Theory, or on technologically deterministic arguments. The focal point of previous scholarship has been more or less to simply justify the 'role' of existing technology in political dissent. It has failed to adequately explain the innovation processes influencing the balance of power in specific case studies. This thesis has attempted to establish a robust, reciprocally valid relationship between online innovations and pro-democracy social movements in a world that increasingly lives its life online. As demonstrated in the next chapter, primary and secondary data collected under this project has been sought in order to address this empirical gap.

Chapter iii: Weblog Content Analysis, Expert Interviews and Document Review—A Methodological Approach Designed for Repressive Contexts

Politically repressive environments are not easy to research due to various access limitations. The third chapter will provide an exhaustive account of the main choices involved, as well as the practical criteria used, in the validation and analysis of data collected through three distinct social research methods.

Methodological Dilemmas: Compassion, Detachment and Self-Reflexivity in Social Research

While pure objectivity remains highly valued by the general scholarly community as a valid theoretical concept (Kortunov and Platonova 2013; Warnick 2011; Westmarland 2001), there are very few socially driven inquiries (Code 2012; Paley and Lilford 2011; Umbricht and Esser 2013) where the researcher(s) can legitimately claim to be fully impartial toward the issues under scrutiny. This is due to the controversial nature of social inequalities, the long-term consequences of which have been occasionally acknowledged in some recent critiques (e.g. Estacio 2012; Yeates 2008) of the existing global social governance regimen.

The opposite end of the spectrum leads us to what can be called intellectual activism (Holmes 2007: 41), which essentially refers to the process of situating oneself within a given instance of social catastrophe. "Only by disorienting the self and uprooting epistemic certainties can anyone hope to inject a positive difference into the unconscious dynamics of the geopolitical order," Holmes reiterates. This particular research technique is, as Maxey (1999: 201) puts it, a pioneering approach to "challenging patriarchal, objectified approaches to knowledge production," verifying that activism and academia do not intrinsically clash in nature, but that they collectively form a new, critical sphere, with which individual inquirers have a chance to critically engage.

The notion of objectivity has been arguably too loosely defined by some commentators and scholars to be constructively applied in politically repressive contexts. Also known as the elite bias, the irregular insistence to actively remove any trace of empathy from crisis-driven studies of the society, will inevitably lead to the production of impractical conclusions and results. In the case of conflict research, as Fine (2006: 91) articulates, there is an ample need to create and promote "collaborative contexts . . . in which we critically think through theory, design, interpretation and use [, and] where we engage in rigorous, collective self-reflection [and] critical distance."

The era of treating activism and academia as two isolated paradigms is long over, and the borders between practice and theory are increasingly blurred – especially as the ICTs become more readily available (Hargreaves 2009) to all. As Pain (2003: 652) reiterates, political activism "exists on a continuum and . . . needs to be accompanied by continuing attention to reflexive research practice."

When processing the results of this research, there were three distinct variables which effectively influenced the ultimate shaping of the analytical framework. A major requisite to meaningful data triangulation in non-positivist research is to examine meticulously the evaluative quality of the data collected through each of the methods involved, which

immediately raises two fundamental methodological questions: a) Who exactly constitutes as an 'expert' in social sciences? b) Where does expert consultation stand in relation to qualitative research? Kaplan (2006: 48) cautions qualitative interviewers about an "ever-growing horde of self-proclaimed experts and generalisers who fill televised panels and print columns without ever having filled up a reporter's notebook," highlighting the rise of a newly emerging breed of social researchers who tend to rely largely on second-hand reporting in order to draw original scholarly conclusions. If nothing else, the undertaking of this thesis has taught me the intrinsic value of first-hand over secondary data, simultaneous to enlightening me vastly on the intricate tasks that are the filtration, validation and interpretation of either type of data.

Indeed, the treatment of online data in qualitative research cannot permanently follow set, prescriptive guidelines, although the general principles of validation remain largely applicable. Thornham and McFarlane (2014: 197) acknowledge based on extensive studies that user-generated content uploaded on the internet is far from static, and that it is a "negotiation, a process of refinement and development", and more importantly a much personalised practice. "If we locate the content as further embedded in a process extending beyond its immediate—spatial, temporal, technological—context" (ibid: 197), it can have considerable bearings on its core value in terms of analytical interpretation. For instance, if a given weblog under longitudinal scrutiny is discontinued, what conclusions can the researcher reach? What if the blog was 'fake' altogether or was 'busted' by the cyber police?

As an avid member and observer of the Persian blogosphere, I have read in 'real-time' many glorious 'posts' which turned out in practice to be the blogger's last words before abduction, imprisonment and in no fewer than two cases 'unexplainable' death. The gradually increasing onslaught of free-to-access information across digital, interactive platforms has led (Livingstone 2004: 6-7) many social scientists researching online media to build their arguments customarily around the question of internet literacy, often avoiding to explore the evolving nature and social implications of the mediating technologies involved. This in turn has contributed to the formation of a "universalist, cognitive framework, thereby neglecting the historical and cultural contingency of both media and the social knowledge processes that interpret them" (ibid: 6-7). Let's consider, for instance, Kelly and Etling's (2008) largely quantitative, computerised approach to cyber-activism in Iran, my idea of responding to which formed the basic theoretical foundation of this PhD. While the authors in question were attempting to explain a dynamically fluid social phenomenon through purely technological values, I found it increasingly necessary to seek a constructivist framework that does not reduce Iran's bottom-up, anti-repression online activists and cyber innovators to passive, reactionary agents, at the same time as explaining the varying limitations of ICTs with regards to social movements.

Activist Research Serving Social Sciences: Bridging the Gap between Theory and Practice in STS

Activist research has been conventionally viewed by many social scientists (e.g. Merton 1936; Varisco 2014) as unmethodical or academically invalid. Therefore, the role of this less recognised branch of qualitative research as a potent catalyst of positive, democratic change is often overlooked (Greenwood 2008; O'Shaughnessy and Krogman 2012; Sclove 1997; Suzuki and Mayorga 2014).

A great example of this theoretical hegemony is the basic philosophical divide between the East and the West in terms of "asymmetries in the terrain of knowledge production and distribution" (Casas 2006: 77), which the new wave of constructivist social scientists aims to reduce and perhaps eventually eliminate in the long run.

Focusing overly on the dismissal (e.g. Walker 1970) of every data collection approach not entirely compatible with conventional social research practices will have a severely negative impact on the scholarly community's basic understanding of the continuously evolving modern-world social unrests. The academia's failure to adequately acknowledge and engage with truly practical fieldwork, according to Choudry (2013: 132), "has made it difficult for social movement theorists to grasp the actual political effects of many movements."

There is a relatively limited understanding in research circles on the potential dangers of getting overly immersed in the pain and suffering of certain repressed groups. However, the general inclination to marry academic social research and outright activism, as Petray (2010: 86) argues, helps "cultural critique to be merged with political action and results in knowledge which contributes not only to academia, but also to the struggle for social justice."

Activism research is widely characterised amongst social scientists by its partiality. However, it would be crucial to understand that the core aim of this branch of research "is not to produce academic theories based on action; Nor is it to produce theories about action; Nor is it to produce theoretical or empirical knowledge that can be applied in action; It is to liberate the human body, mind and spirit in the search for a better, freer world" (Reason and Bradbury 2013: 5) – a philanthropic approach pursued by this research in terms of alleviating the counter-democratic restrictions imposed on Iran's cyber-activist community.

On a broader level, the common speculation that academia, activism and policy in nationwide contexts are by default in tune with one another is far from realistic. While empirical evidence, as Barreras (2004: 5) argues, plays an "important and perhaps necessary role, [it] is often not enough to promote policy change." There is now an ever increasing need to recognise the overlooked principle that when stimulating social transformations of profound magnitude, there is simply not such a direct answer as establishing a functionally shared communication channel between academia and politics. An effective solution to this paradox, as Hale (2008: 16) recaps, is to ensure fostering "collaboration and communication with those whose work in NGOs, social movement organisations, businesses, legal advocacy, and other arenas that can be improved by social science knowledge—and can challenge social scientists to keep improving their own understandings."

Today, one of the most progressive ways in which one can contribute to the literature on modern social movements is to develop a comprehensive framework aimed at promoting a stronger and more sustainable link between activism and academia which will, in Carpenter's (2009: 217) terms, subsequently help "translate activism into liberatory classroom pedagogies . . . , [which can in turn] empower people in our communities." Without fully implementing this mutually constructive (Woodhouse et al. 2002) theoretical framework, the likelihood of reaching a co-beneficial medium is relatively dim. Thus, it is increasingly crucial for leading universities in the industrialised democracies to treat Social Sciences in such a way that the discipline recurrently "renews itself through direct engagement with practical problems and efforts to create a better world" (Hale 2008: 17). Scholarly researchers are (ibid: 22) fully capable of helping "activists reflect on their own movements and struggles, partly through

knowledge of how other struggles have played out, [. . . bringing] knowledge of tactics to expand the repertoires of activists."

Reflexivity in social research goes significantly beyond a static justification of choice. Despite the common perception that it is passive or reactionary, self-reflexivity is "a defining feature of human consciousness in a postmodern world – a challenge to conventional ideals of science which favour professional distance and objectivity over engagement and subjectivity" (Finlay and Gough 2003: 1). Adhering to this dynamic analytical framework has resulted in this research to transform from an initially linear mission to a highly rewarding learning process. When we in social sciences reflect on our strategies, we are simply acknowledging a constructive awareness of our inadvertent influences as a scholar on the trajectory of our research. It is this so-called postmodern sensibility, as Finlay and Gough (ibid: 1) argue, which "compels us to recognise and celebrate diverse, shifting and often contradictory self-fragments – to be playful and detached rather than engage seriously with questions about true or enduring values."

Perhaps the most invaluable contribution made by the self-reflexivity process to this research was the formation of a broader understanding of the scope and nature of practical restrictions by which its methodological choices were characterised. As Spencer and Ritchie (2012) observe, it happens all too often that researchers "support their findings only with extracts of raw data without illustrating how their analytic output was constructed."

Like many other social projects, this research was initially designed based on a largely linear hypothesis. Nearly half a decade on, what was resulted was a comprehensive range of relatively far more sophisticated insights not only into the social processes involved in online censorship in Iran and other repressive states, but more importantly, those into the intrinsic challenges associated with the qualitative studies of political repression in general. It is, in the opinion of Yardley (2000: 224) vital that the "diversity and mutability which are central to [social research] approaches is preserved despite the difficulties this may create for the process of communicating the nature and merits of different qualitative methods, and developing procedures for verifying the excellence and integrity of research employing [them]." In all honesty, researching Iran's online censorship apparatus, despite its very many intellectual rewards, has raised more questions for me in terms of political repression than it has so far addressed.

The criteria employed to analyse the results of this research were drawn from a selection of prominent social research textbooks, although there were admittedly a degree of political influences involved. These influences were largely owed to my personal sympathy, if not an outright sense of belonging, towards Iran's Green Movement, which was in hindsight integral in the project's choice of data sources (i.e. blogs, interviewees, media accounts), as well as its design and use of tailored checklists and questionnaires. For example, it can be argued that the snowball sampling of the activist Persian weblogs and interviewees resulted in the conclusions to be partially biased, or that too many of the interviewees relied excessively on left-oriented published material or media reports, many of which had been already taken into account directly by this research.

All these choices and dilemmas made the projected plans for a robust data triangulation more challenging to execute, if not impossible. As Tracy (2010: 838) argues, even when interpretive measures in social research are entirely founded on scholarly justifications, their practical "consequence of any delineation of criteria" is almost invariably political. "Tools,

frameworks, and criteria are not value-free. By offering an answer to 'what makes a qualitative research study good,' [we must also] thoughtfully attend to the long history and controversy that swirls amongst the politics of evidence," she elaborates. The Iranian society at large is one characterised by strong popular "support for pro-liberal values such as a belief in the importance of self-direction and benevolence" (Porat 2012), as well as by an "uneven development of capitalism and industrialisation" (Tohidi 1991: 259). Before one can rigorously evaluate the data collected from the field, it is imperative that such influential socio-political variants are identified, understood and embedded into the grand scheme of the analytical criteria. This study would not have taken place if I were not as intimately familiar with, as well as genuinely concerned about, the socio-political issues underlying the questions raised regarding the case study under scrutiny. But more importantly, the very same personal circumstances and emotional commitments under which this research was conducted were to some degree influential on the reliability of the end results. Thus, the key idea here is not to focus merely on the notions of access or prior contextual knowledge, but also on one's ability to objectively identify, keep up with and process in time a steadily inflowing stream of evidence on the highly dynamic subject that is online communication, and during or in the aftermath of a major political turmoil. Of course, this may well involve various uncomfortable yet sensible decisions and compromises in one's personal ambitions and political beliefs.

Not too long ago, when I was presenting a paper extracted from this thesis at an international symposium on media and democracy held at the London School of Economics and Politics, a senior colleague sitting on the panel told me that she thought I was overstating the case of gender gap in Iran, which she said in her opinion was not necessarily at odds with 'normal realities' of a non-Western society. Many months on, I am yet to make utter peace about how epically distant our perspectives were. As Eyben (2015: 4) explains, upholding a pragmatic, multi-disciplinary discussion surrounding the so-called politics of evidence is "mutually beneficial and help re-imagine and reconceptualise" the global promotion of human development. Without such a constructivist discourse, the horizon of activist scholarship will remain unpromising to say the least. In Denzin's (2009: 155) view, there is a sizeable breed of research analysts that regards "dispassionate objectivity" as an ultimately ideal practice. "Global efforts to impose a new orthodoxy on critical social science inquiry must be resisted. A hegemonic politics of evidence cannot be allowed. Too much is at stake", he firmly asserts.

So how exactly can we define a framework which not only openly includes experts from various academic disciplines and political backgrounds, but also more vitally enables constructive discussions amongst them with the distinct aim of creating a fairer society? According to Morse (2006: 395), evidence in social research is made of "concrete and indisputable" facts, while politics can be described as "activities concerned with the acquisition or exercise of authority [and are] necessarily ephemeral and subjective." During the course of this research, there were countless instances where an observed weblog diverted abruptly to highly offensive language and other contents due to what I assessed at the time to be frustrated radicalisation. Although arguably understandable in context and given the surrounding circumstances, the response of this research was almost invariably to eliminate the blog in question from the final shortlist. As this project sees it, leaving extreme ideological views out of the equation will have to be the only sustainable solution to creating a common ground that serves and unites all the reasonable inhabitants of a modern, civilised community. I also would like to refer to the ethical principles underlying my initiation of this thesis as an 'operational bottom-line', which I hope can help further fade the traditional lines of division between classic scholarships and academically validated activist research.

Hindsight Reflections: Deconstructing the Research Design in Retrospect

From a methodological perspective, the overall results of the project at hand have largely served to uncover new insights to the increasing significance of online observation (Bengry-Howell et al. 2011) and networking (Hine 2007; 2011), as well as to help justify the circumstantial integration of activist spectacles with institutionally approved social research techniques (Bryman 2012).

The sampling of the Persian activist weblogs was planned in such a way that they came entirely from the 'opposition' camp. This was not to cut any methodological slacks, but rather an organised attempt to give an otherwise unheard voice to a relatively sizeable political class systematically oppressed since June 2009 (Dabashi 2011; Milani 2010; Tahmasebi-Birgani 2010). The blogs were seen primarily in the research design as direct, first-hand sources of raw information on the Iranian activists' engagement with new ICTs. Although every effort was made to validate the true identity of the bloggers, a scant minority remained somewhat inconclusive. This has been carefully considered during the analysis phase to ensure minimum impact on data authenticity. For instance, in the few cases where the true gender identity or the exact geographical location of the blogger could not be confirmed beyond reasonable doubt, vigilant care was taken to ensure their exclusion from all processes relating directly to the corresponding analytical dimension.

While the sampled interviewee population reflects three distinct categories of experienced professionals, it too excluded informants with any past or current known links to the inner layers of the Iranian regime. This was mainly to help give a voice to the oppressed progressive currents, and to minimise the presence of any ideological or fear-driven bias. Among autocratic states worldwide, Iran's online police have a particular reputation (Lock et al. 2013: 5) for their "threats against Iranians outside the country who are disenchanted with the current government, in some cases leading to detainment and arrest." Setting aside the ethical restrictions imposed by institutional regulations, there would have been no viable route to methodically obtain and assess the true insights held by top IRGC operatives from an academic perspective.

The formal documents reviewed throughout the thesis were selected on a largely inductive basis, meaning that their inclusion was influenced significantly by the social patterns emerging from the preliminary data analysis. Some publication categories retrieved specifically for this project include recent credible studies of the Iranian NIS, country-specific statistical data based on leading humanitarian NGOs' research, relevant scholarly journal and conference papers, investigative reports conducted by prominent news agencies, and official analyses, correspondences and statements released by political institutions and specialised think tanks in Europe and North America.

The main aim of this study being philanthropic (as opposed to politically motivated) in nature, the verified facts extracted from published documents played a big role in validating the refined data toward the final stretch of the pre-analysis phase, as well as being highly helpful in detecting empirical patterns which could have otherwise remained concealed. This aspect of the grand methodology has also been instrumental to drawing and justifying the final conclusions – a dynamic approach to qualitative research associated (Adham et al. 2015) closely with some of the most impactful scholarly campaigns for the promotion of human rights in the relatively young (O'Lear 2015) history of STS.

The research methods implemented throughout this project were exclusively crafted to serve one crucial end: evaluating the project's core hypothesis on the socio-technical dynamics of online innovation among politically progressive Iranian cyber-activists, alongside that of the regime's censorship apparatus. While analysing the content of the weblogs proved significant to both identifying and explaining the forms of online protest in Iran, the semi-structured interviews facilitated the factuality verification process by providing the framework with an invaluable set of expert consultations. Finally, the critical review of a relatively large volume of officially published online and offline documents revealed an array of essential facts, figures and statistic, in addition to contributing extensively to the understanding of the hidden subtleties of Iran's cyber-activism scene. On an opposite note, the time limit factor driven by personal commitments and circumstances, the lack of sufficient financial resources, and also the access issues rooted in ethical and safety concerns raised by the host institution were to some degree influential on the general outcome of this thesis. Of course, the successful elimination of each of these operational obstacles could have possibly helped further improve the overall quality of the produced results by enhancing (Wilkinson 2005) analytical precision.

Research Methods: An Overview

The complexity of STS has been routinely undermined by loyal adherents of technological determinism. Socio-technical Systems, as Reddy (2013) argues, best benefit from qualitative research methods—particularly useful for "examining complex environments where technical, organisational and social factors intersect." Much social research in academia employs quantitative data collection methods, often ignoring the interpretive nature of the discipline out of convenience. This creates distraction in the scholarly literature, as such research typically "fails to communicate information clearly or efficiently" (Callahan 2006: 73) at least in certain subjects.

The methodological design of this project has been developed carefully to complement both the theoretical framework within which the study is conducted and the sophistications required to research repressive countries like Iran. It takes into account the ethical issues which can arise as a result of such inquiries. Given that the main conceptual foundations of the research at hand were originated in the Northern European states, it was important to demonstrate the structural differences at work here. Thus, the sources of data were systematically categorised to help explain the reciprocal correlation between political developments and ICT innovations in Iran, with the hope that this may help establish a general model to serve other emerging economies in the world.

To ensure the reliability and accuracy of the research, three distinct data collection methods were adopted, putting the main emphasis on first-hand data collected in relation to Iran as the primary case-study, at the same time as enabling systematic triangulation of the results.

The following graph shows the chief sources of data employed by this project:

Research Methods: A Tailored Design for a Repressive Context

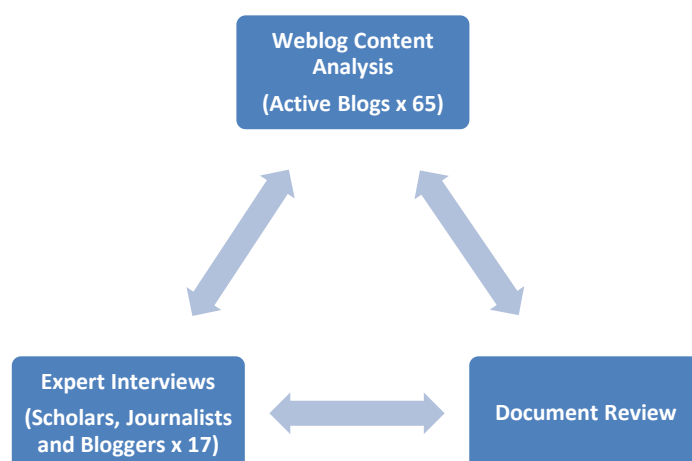


Figure 12

The core dataset of this study consisted of the following four general categories:

- Evidence of the structure and functions of Iran's NIS, of its reliance on foreign technologies, and of the contribution of Western ICT companies to online censorship in Iran. Sources include scholarly journals and print/broadcast/online media outlets.
- Evidence of regime-sponsored hacking attacks aimed at cyber-activists as well as evidence of censorship of their efforts and proof of the regime's overall cyber-power. Sources include Persian weblogs, technical press/journals and semi-structured interviews.
- Evidence of hacking attacks against the regime conducted by local and expatriate Iranian pro-democracy activists as well as evidence of the systematic use of anti-filtering software developed inside and outside Iran. Sources include Persian weblogs and semi-structured interviews.
- Key texts of international export policies for dual-purpose ICTs as well as evidence of consumer boycotts launched against Western telecommunications technology companies that contribute to online censorship in repressive states. Sources include official documents published by respective authorities, scholarly journal articles and media accounts.

Weblog Content Analysis

This research has generated a set of data on Persian cyber-activists living inside and outside Iran, taking into account factors including location, gender, education and technological innovativeness. The main purpose of this data collection phase was to help assess the computer literacy and innovation capabilities of politically active Persian bloggers, as well as the extent of their reliance on foreign anti-censorship software.

Despite the increasing popularity of online social networking, the blogosphere remains the most prominent form of pro-democracy cyber-activism in Iran—the youngest and most

highly connected country in the Middle East (BBC Persian 2013) and the second largest blogging nation in the world (Vakil 2011). Although modern cyber-activism in Iran has roots that stretch back into the late 1990s, it was radically transformed following the disputed presidential election in June 2009, when the regime's heavy-handed suppression of street protesters made ICTs even more relevant to political dissent. The booming number of politically motivated Persian blogs makes them a suitable tool for measuring cyber-activism in Iran and a symbolic mirror reflecting bottom-up technological creativity. In this social movement entirely reliant on ICTs, online innovations are the metaphorical blood in the cyber-activists' veins. They should be most visible where the power struggle is fought the hardest.

Having examined hundreds of Persian blogs on a longitudinal basis, 65 were eventually selected for close monitoring, in a bid to identify and explain the main patterns in the Iranian cyber-activists' experiments with online innovation. The blogs were carefully sampled from a wide range of options, bearing in mind the following criteria:

- **Degree of popularity:** Determined in a number of ways, including observing unique hit counts and/or taking into account the volume, scale and dominant tone of the user comments left on each post.
- **Keyword frequency/relevance:** Only blogs which actively contributed to the online power struggle with the regime were selected. Selection criteria involved developing an extensive, context-driven list of Persian keywords known (see Kelly and Etling 2008) to be closely associated with the pro-democracy discourse within the Persian blogosphere.
- **Regularity of updates:** As a general rule, only blogs whose content frequency did not fall under the threshold of one post per two weeks were chosen. This was mainly to avoid wasting time on short-term, casual activity, and to ensure that the sampled blogs were worthy of analysis.
- **Location diversity:** The blogs were sampled equally from across an array of websites maintained both inside and outside Iran, in order to help analyse and potentially distinguish between local and expatriate cyber-activists' innovativeness in relation with the online power struggle with the Islamic regime.
- **Background diversity:** In order to strengthen the reliability of the results of the research, the selected blogs were chosen to represent a well-rounded range of mainstream netizens. No socio-political class was allowed to dominate the sampling range.

Many well-known political bloggers use a 'sidebar,' where they recommend one another's blogs to their visitors, creating a massive network of interlinked, likeminded cyber-activists. This facilitates browsing through homogeneous blogs and aids the systemisation of sampling. The two hundred blogs initially considered were gradually narrowed down to one hundred and twenty, of which fifty-five were later eliminated for at least one of the following reasons:

- **Lack of sophistication:** As the Iranian government increased its pressure on online dissidents, a number of anonymous anti-regime blogs made excessive use of obscenities. Such sites are often created not by 'genuine' cyber-activists, but instead

by frustrated youngsters turning to derogatory language as a means to release psychosocial pressure.

- **Gradual change of focus:** Many young political activists residing in repressive countries have an inclination to use blogging websites as a temporary platform to practice citizen journalism—an impulsive reaction to political violence. These blogs soon tend to either take other, non-political directions or even stop updating altogether, as soon as a major flashpoint is over.

The blogs were analysed using a carefully composed checklist consisting of seven distinct questions:

Blog Analysis Checklist

Question	Objective
1. What is the location of the blogger?	To help explain the different ways local and expatriate Iranian cyber-activists contribute to online power struggles with the regime.
2. What is the gender of the blogger?	To help clarify differences between how male and female Iranian cyber-activists contribute to the country's system of online innovations, as well as to help measure the male/female representation ratio within Iran's NIS.
3. What is the main focus of the updates?	To help look for discussions related to the use of technology by Iranian cyber-activists, and the contribution of foreign telecommunications companies to the regime's online policing activities, etc.
4. Does the blogger use their outlet as a means to circulate protest/petition/strike calls?	To help find examples of consumer boycotts against foreign telecommunications companies and their influence on lobbying for export controls
5. What level of computer literacy does the blogger exhibit?	To help understand how the regime's restriction of online communications has been countered by the cyber-activists' innovations, and the extent to which these innovations have succeeded

6. Does the blogger use their outlet as a means to share or obtain technical tips about countering the regime's repressive technology, such as how to bypass internet filtering, un-jam satellite TV signals, protect online identities, increase network security or launch hacking attacks on the websites associated with the regime's online police?	To gather specific data on circumvention techniques used by cyber-activists
7. How many regular contributors does each blog have?	To help evaluate the ability of online technologies to unite like-minded cyber-activists through enabling and encouraging teamwork

Table 3

Expert Interviews

Semi-structured interviews were used because they are flexible in nature, making them suitable for comparison-driven contexts where "more than a few of the open-ended questions require follow-up queries" (Adams 2010: 367). Convenient, low-risk access was another crucial factor behind the selection of Western-based specialists in preference over those directly involved in the crisis. The interviews enabled the collection of an essential dataset on the online power struggle in Iran, as well as on the structure and functionality of the country's NIS, helping to test the hypothesis of this research as well as answer its main questions. Highly experienced in their respective fields, the participants were viewed as professional consultants, whose insights proved valuable to the verification of the blog findings.

Structured interviews generate quantitative results, making them unsuitable for qualitative research. The significance of semi-structured interviews to qualitative research is that the method facilitates informed interpretation—valuable in social research—and consequently allows for more in-depth investigation. This makes it possible, as Barriball and while (1994: 330) explain, for the same question to be rephrased over and over again, refined to be more fitting for participants with various understandings of certain terms or concepts. As they put it, in semi-structured interviews, "validity and reliability depend not upon the repeated use of the same words in each question, but upon conveying equivalence of meaning. It is this equivalence of meaning which helps to standardise the semi-structured interview and facilitate comparability." Given the professional diversity of the population of interviewees in this study, only a semi-structured approach could deliver the refined results typically demanded by a post-graduate research project of such vast scope.

Seventeen experts were interviewed in total. The informants were chosen based on the chain referral or 'snowball' sampling method. They comprised a range of prominent figures, divided into three distinct categories of bloggers/activists, scholars and technology journalists. Snowball sampling is particularly beneficial in identifying and explaining relationships and characteristics important to a specific community in regards to an explicit research topic (Atkinson and Flint 2001; Biernacki and Waldorf 1981). All the participants were fully briefed on the aims, objectives and likely future implications of the research; none objected to the public disclosure of their true identity in the final dissertation. The mode and length of the interviews varied due to several factors such as the participants' availability. No electronic recording of any kind was involved during the entire process, in order to both encourage honesty and avoid ethical complications. The majority of the conversations were conducted

in person, but alternative means of communication such as regular telephone, Skype and other secure online chatting services were also employed on a few occasions due to timing and/or accessibility issues.

The interview material for this research was gathered in person (i.e. face-to-face discussion) as a general rule, although there were multiple instances where follow-up questions and clarification requests were communicated to some of the interviewees through email, telephone or Skype. In order to maintain ethical integrity, it was decided at the outset to not record any of the interviews electronically. Instead, shorthand and other personalised coding and summarising techniques were used to document the participants' comments and answers. The full interview transcripts were later on assessed in relation to a checklist developed based on analytical dimensions emerging from the activist Persian weblogs and published documents, and with careful attention to the core expertise of every informant. Where shorthand was employed, reasonable care was taken to preserve the integrity of the provided responses, by revisiting the interview notes in a disturbance-free physical setting and immediately following the event. Also, in many instances the full edited scripts were shared in writing with the respondents, who almost consistently confirmed their general satisfaction with the conceptual authenticity of the quotes. Where there were issues raised, amendments were made upon request.

The following table shows a list of the core questions provided to the interviewees, as well as the research objective each question specifically serves:

Interview Questions

Question	Objective
1. Where do you place social networking and politically motivated hacking attacks in the online power struggle between the regime and the cyber-activists in Iran?	To help determine the relationship between online innovations and political processes and underline the technological elements contributing to repression, as well as those encouraging democratic activity
2. What is the contribution of the government / IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship / surveillance infrastructure?	To help clarify the Defence Ministry's / IRGC's extent of influence on the regime's innovation policies and strategies in the field of online technologies
3. To what extent is the Iranian regime self-reliant in terms of producing censorship / surveillance technology? Why?	To help explain the structure and functionality of the Iranian regime's system of online innovations
4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of the cyber-activists in Iran?	To reveal if foreign telecommunications technology companies have helped address the issues faced by the Iranian regime with regards to its system of online innovations and the extent of this assistance
5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?	To help better regulate the export of dual-purpose telecommunications technologies by foreign companies to repressive countries such as Iran

6. What are the main anti-censorship / surveillance methods used by Iranian cyber-activists? How widespread are such practices?	To help identify the main sources of the software currently used by the Iranian cyber-activists and explain the innovation processes leading to such technologies
7. What are the main sources behind the development of the anti-censorship / surveillance software currently used by Iranian cyber-activists?	Same as above
8. How do you differentiate the local and expat Iranian cyber-activists' role in their power struggle with the regime?	To help distinguish the different ways in which local and expatriate Iranian cyber-activists have influenced processes involved in the invention of anti-censorship/surveillance technologies

Table 4

Document Review

Aside from its grounding in the scholarly literature, this research also chose to assess a series of official documents as part of its analytical framework, a full list of which can be found under appendices.

These documents include journalistic accounts and editorials published in credible mainstream news media (e.g. BBC, Bloomberg, New York Times, Wall Street Journal, etc.) and legal statements issued formally by the EU, UN and US authorities, with a special focus on official declarations reflecting the West's latest policies on the trade of ICTs with the Iranian regime. In addition, a series of relevant online and offline public communications were examined, such as NSN's press releases issued in response to the allegations of business misconduct in Iran.

Analytical Framework

The data collected for this research has been analysed using manual qualitative techniques.

With regards to the Persian blogs, the results were initially broken down and laid out in MS Word tables, in accordance with the provided checklist. These were then rigorously scrutinised for emerging patterns in the use of online technologies, bearing in mind a combination of demographic, cultural, social and psychological variants. These patterns were then reviewed and translated into a range of simplified, relatable charts and graphs, using MS Excel and Adobe Photoshop.

Regarding the interviews, an inductive analysis was performed on the raw transcriptions to help detect patterns that could help validate or dismiss the hypothesis and to answer the main research questions. A carefully filtered extraction of the interviewees' answers was outlined, processed and visualised in the same fashion as the blog contents.

Weighing the above two datasets against one another significantly facilitated the analysis: unsubstantiated arguments were eliminated, boosting the accuracy of the proposed claims.

The refined outcomes of the preliminary and secondary stages of data analysis were then finalised by being passed through a fact-checking framework, consisting mostly of published scholarly and journalistic documents.

In order to assure robust results, conclusions were based on the outcome of this triangulation process. A copy of the analysis tables and formulas can be found under Appendices.

Ethical Clearance

Formal approval of the University Research Ethics Committee (UREC) was granted on 5 October 2011 (See Appendices for a copy of the certificate).

With regard to the blogs analysed, no private or public contact was conducted with any of the bloggers at any stage of the study, and the true identity of the bloggers was kept fully hidden unless disclosed via a public profile page. The emergence of the online sphere has unsettled the principles of qualitative research, causing a multitude of complexities over the past two decades, especially in the field of Social Sciences (Masson et al. 2013). Yet there is no real reason why the internet should not be treated similarly to its offline equivalents, except in a few infrequent enough instances. Data willingly posted on a communal domain, where authors cannot typically choose their audiences, can legitimately be treated as public, especially as this domain is commonly known to be communal and to operate in this manner. Eysenbach and Till (2001: 1104) insist that informed consent is a necessity, "when behaviour of research participants occurs in a private context where an individual can reasonably expect that no observation or reporting is taking place." Privacy, as Kuper et al. (2008: 689) argue, becomes an ethical issue only "when data constitute personal reports of experience or perception," and it would be safe to suggest that overtly presented political arguments do not fall under the category of confidential data. Nonetheless, any technical details likely to help divulge the bloggers' true identity were removed from the final manuscript.

Although the preliminary methodological framework of this thesis was designed to rely mostly on first-hand data, reported data (i.e. media accounts, expert interviews, etc.) became increasingly integral to the research process, due to various access issues amongst others. This subsequently had profound theoretical implications for the end results in terms of both analysis and validation. As Jick (1979: 608–9) assesses, primary—or directly collected—data can be central to the quality of analysis in a social research project. "While one can rely on certain scientific conventions for maximising the credibility of one's findings, the researcher using triangulation is likely to rely still more on a 'feel' of the situation . . . Situational factors play a prominent role [in illuminating behaviour in context]," he argues. Such unfiltered experience of the matters would have been empirically invaluable to the authenticity of this project, by assisting to provide a considerably more in-depth explanation of how Iran's cyber-activist network of innovation functions and communicates.

Nonetheless, the resulting void within the core dataset was rectified to some extent through admitting a systematically vetted repertoire of published documents and reports. According to Hox and Boeije (2005: 598), researchers working with secondary data must consider carefully whether the data appropriately fit their research question. "In general, it is acceptable if the limitations of the available data limit the secondary analysis to some extent, for instance, by impeding tests of some specific hypothesis. However, it is not acceptable if the limitations of the data make it necessary to change the research question in order to be able to use them at all," they emphasise. Perhaps the main intellectual lesson arising from the

extensive employment of secondary sources for this thesis was learning to differentiate in practice the 'impossible' and the 'unlikely' in academic social research, and more importantly to vigilantly look out for and try to manage efficiently any instances of previously unfathomable data-hypothesis clash, where the truth is "sometimes uncomfortable" (Lieberson 1989: 60). After all, the final verdict was clear: despite all the positive contributions and outcomes, the idea of gaining a fully comprehensive insight into Iran's most secretive layers of political opposition from afar was a socio-technically ambitious one to say the least.

Secondary data can often make it much more difficult for the researcher to monitor and preserve the quality of the results. Social research involving secondary reporting usually dictates that "additional information [are] archived with the data itself . . . [and] to make certain that such additional metadata describing the data and their quality are in fact available" (ibid: 598). This is particularly noteworthy due to the characteristically tempting nature of philanthropic inquiries, which can easily lure the researcher into gathering a far larger quantity of raw data than a self-funded, independent academic project is typically capable of processing. Consistent with the argument of Hox and Boeijs, this thesis resonates widely in hindsight with Greene's (1995: 16) search for a formal model of social science data and its analysis, "which can directly guide the design of documentation and metadata." Although viewed initially by this project as a productive strategy reassuring accuracy, soon organisational challenges began surfacing as a result of data overload, somewhat disrupting the projected completion timeline of the thesis. The most recently occurred example of this methodological chaos was an unforeseen, urgent need to revisit a large portion of the published materials referenced throughout the dissertation, which proved to be highly troubling due to a lack of proper archiving, as well as to the ephemeral nature of online content.

In terms of source protection, the interviewees consisted only of Western nationals and expatriate Iranians, all of whom were fully briefed. They were also informed about their right to withdraw from participation. All gave their informed consent to inclusion in this research.

Finally, the documents reviewed for this research were all openly published legal communications downloaded from certified websites, the scrutiny of which is highly unlikely to raise any ethical complications for individuals or institutions involved.

A triangulated, thorough analysis of the main research findings follows in the next chapter.

Chapter iv: Democratic Structure, Bimodality and NIS—A Triangulated Analysis of Innovation Patterns and Processes within Iran's Online Sphere

The following chapter aims to present and analyse key findings of the research in light of the hypothesis. This will include empirical evidence of the bimodality and dysfunction of Iran's National Innovation System when compared to Freeman and Lundvall's classic NIS model, as well as the existence of socially shaped innovation patterns within the country's cyber-activist community. I will then explore a proposed, alternative model of national innovation and examine its potential transferability to other politically repressive environments on the basis of a set of indicators such as gender equality, geographical location of cyber-activists and democratic features of the given innovation systems in individual countries. These indicators were identified through blog content analysis, expert interviews and document analysis.

Activism in Iran: Where Do ICTs Stand?

While the structure and functionality of an NIS does not automatically dictate the balance of power in a repressive country, it is an accurate determinant of various influential actors' potential competence in the hostile, often highly divided political discourse existing in such states. The separation of Iran's NIS into two isolated, disproportionately funded sub-systems is likely to have disrupted the fair distribution of the means of research and development in the country, preventing healthy, merit-based competition and collaboration among the institutions, enterprises and universities involved. The half of the country's NIS loyal to—and supervised by—high-ranking security officials within the regime has been weakened by the bimodality of Iran's NIS, along with Western trade restrictions and sanctions, depriving it of an irreplaceable source of domestic scientific expertise.

A similar case can be made for the other half of the NIS—taken to consist of politically more moderate, pro-democracy schools of thought inside and outside of Iran. Apart from explaining Iran's largely under-documented NIS, this analysis can be used directly in the scrutiny of the effects of imported technologies on the regime's ability to repress political dissent, as well as to cyber-activists' counter-repressive abilities. Hence, it can be used when seeking to influence the balance of power in the country's highly polarised online political discourse, where an increasingly intense clash of interests is currently in progress.

Iran has not only the youngest and most highly educated population in the Middle East but also the highest rate of connectivity in the region. These factors, along with dissatisfaction of Iranian middle class youth at the regime's stance on civil liberties as demonstrated in the street protests in 2009 as well as in the landslide victory of the only non-conservative presidential candidate in 2013, have made the internet a key sphere for dissidents.

Online media have now moved to the frontline of the country's political discourse. As shown in the table below, about three quarters of the interviewees believed that the internet as a medium has a role in the conflict in question, while only one contested the significance of online technology.

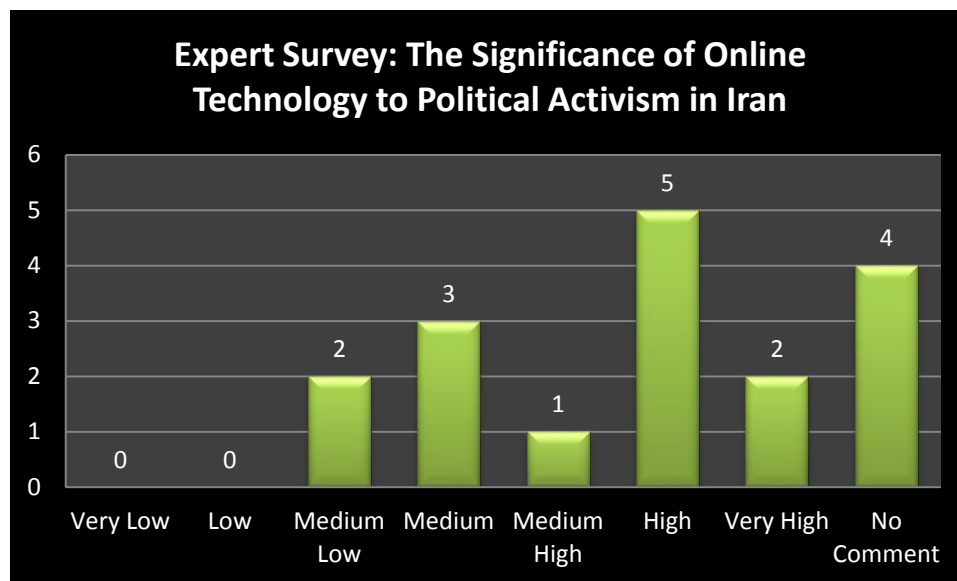


Figure 13

The only respondent who largely discounts the importance of online communication methods to the power struggle in Iran is Dr. Randy Kluver, Associate Professor in the Department of Communication at Texas A&M University and Executive Director in the Office of International Affairs there, who thinks that on its own, "social networking is not all that important," except for its ability "to develop networks of resistance." With regards to hacking attacks, he believes that they are "primarily symbolic, and [have] no real function other than to say 'we were here.'" This comment tends to capture the essence of the constructivist approach toward cyber-activism and supports the case of the critics of technological determinism such as Mackenzie and Wajcman (1985), the developers of the Social Shaping of Technology theory, who suggested that the way technology affects society is largely a consequence of the way the society itself relates to technology and is, therefore, context-driven. They argue that this, in turn, influences the direction and pattern of future technological innovations in a given field.

Although a dominant majority of the participants confirm the significance of online media to political developments in Iran, there seems to be a divisive disagreement amongst them with regards to how ICTs influence activism and the nation. Dr. Alexander Dawoody, Assistant Professor of Public Policy at Marywood University, sees cyber-activism as merely useful to the Iranian diaspora with very limited domestic capacity to effect change. On the other hand, Elahe Boghrat, a journalist at the London-based online newspaper Kayhan, finds both online social networking and hacking attacks to be greatly useful to the Iranian cyber-activists, "as online activism does not usually lead to torture and violent death." Dr. James Fielder, Air Force Major and scholar in International Relations and Comparative Politics, observes that social networking has much more weight than hacking attacks in Iranian contexts and states that even when hacking attacks are employed they are "used to evade censors rather than to carry out offensive attacks," elaborating that "maintaining reliable communication channels appear[s] more important."

Dr. Tessa Houghton fully agrees with the statement that social networking sites represent a greater potential threat to the regime than hacking attacks, as "they have the potential to facilitate organisation and solidarity amongst much greater numbers of people than single instances of . . . DDoS or defacements." Layla Hashemi, Professor of History and Political

Science at Montgomery College, Nassim Nazemi, Juris Doctor and Law Clerk at the United States Court of Appeals for the Ninth Circuit, and Kevin Coleman, Senior Fellow at Technolytics Institute, all see the internet as a key component in Iranian politics and of great value to Iran's civil rights movement, as it is unbound by geographical specification. Mr. Coleman goes on further to rate the influence of both social media and hacking attacks on political activism in Iran:

Social Networking Sites (1 = Low, 3 = Medium, 5 = High):

- 4.0 with a potential of 4.4

Hactivism (1 = Low, 3 = Medium, 5 = High):

- 3.5 with a potential of 4.2

Other experts expand the focus beyond the cyber-activist zone and discuss online innovations in a broader context inclusive of the government and pro-regime activists. The overall view of Dr. Jed Crandall, Assistant Professor of Computer Science at the University of New Mexico, is that the internet is ultimately in service of repression, briefly explaining that "the government could be using man-in-the-middle attacks to steal [a cyber-activist's] username and password and then monitor their activities and tie particular people to specific social media posts." If this claim is true, then the scholarly community will have very little choice but to conclude that the online sphere is not a significant or even suitable communication method for political activism, as counter-innovations will hardly have any significance in an environment where the oppressive force inevitably has the upper hand.

Neal Ungerleider, Social Media Consultant and International Technology and Cyber-security Reporter at Fast Company, argues that social networking is primarily useful to the Iranian activist diaspora and their sympathisers, adding that "DDoS, malware and phishing attacks against cyber-activists are common at the hands of the Iranian government and regime supporters." This portrayal, which assigns social networking to the activist groups and hacking attacks to the repressive force, is one that particularly underlines the role of social processes in systematic innovation. If we assume that repressive regimes have small popular bases within the nations they rule, we can see why they need to invest a relatively disproportionate amount of resources in top-down, commissioned technological innovations. This stands against the crowd-sourced, bottom-up and more democratically driven innovation system established in the activist community, which is primarily empowered by concepts such as social collaboration, virality and dark humour, as well as a non-specialised and often experimental foundation of ICT-mediated networking knowledge, all tied together by a shared sense of motivation rooted in a common political goal.

Taking into account Boudreau and Lakhani's (2013: 7) argument that "crowds . . . are energised by intrinsic motivations . . . that are more likely to come into play when people decide for themselves what problems to attack," the Persian online sphere must consist of motivated individuals who have, out of necessity, resorted to acquiring knowledge that could potentially help them with day-to-day technological challenges they face on the internet as a result of the Islamic Republic's censorship policies. This configuration and situation has resulted in the formation of what this research calls a Cyber-activist Innovation System (CIS), characterised by its sharp focus on anti-censorship activities. The existence of such a community network is particularly manifest in the recurrent appearance of a 'recommended bloggers' sidebar on politically active Persian blogs, revealing the depth of interconnectivity among Iranian cyber-activists.

Dr. Ulises Mejias, Assistant Professor of Communication Studies at the State University of New York at Oswego, does not deny the ability of social networking tools to organise activism and disseminate information, but believes that this mode of cyber-activism is not as directly confrontational as politically motivated hacking attacks. He, however, argues that the importance of cyber-activism might be slightly overrated "in Iran, where the government has at its disposal the same tools other governments have to monitor, track, and block online activities, but is willing to use them more overtly to stifle dissent." Madeline Storck, scholar in International Relations and Affairs and in Media and Communications, agrees and further criticises the media's tendency to use unscientific terms such as "Twitter revolution" or "Facebook revolution" when referring to the popular uprisings in the Middle East. She suggests this trend "relies on broad assumptions about the democratic nature of the internet, ignoring the importance of context, both cultural and historical," particularly in Iran, where the regime "is known to have one of the most advanced systems of networked authoritarianism in the world, perhaps second only to China."

The above findings underline the importance of innovation processes in shaping the balance of power in a repressive state such as Iran. Moreover, they justify the new theoretical framework proposed by this research. While most studies about the issue focus on conventional, static anti-censorship techniques common in cyber-activism, the contextual realities in Iran reflect a rather different portrait. The research at hand shows that not only are the majority of the users alien to advanced anti-censorship technology, but also that the regime continuously detects and disables such tools with various borrowed filtering techniques.

Anti-Censorship Innovations: How Do They Emerge?

The dynamics of innovation in both of Iran's NIS modes are interconnected. If we examine the conflict from a pro-democracy perspective, we see that Iran's cyber-activists play off the regime's oppressive policies, acting primarily in reaction to its moves. Their main endeavour is to reclaim universally recognised civil rights of free speech and the right to information. The regime, by making ideology-driven technological choices with typically repressive repercussions, drives the conflict against itself and remains responsible for intensifying a fire already consuming the country's resources.

It must be noted, however, that online proxies known as anonymisers have never really been a fully viable solution for Iranian activists, due to many limitations they have as well as to the generally very slow speed of 'broadband' connections in Iranian homes. That is why Virtual Private Networks (VPNs), or cheap sources of "tunnelling, encryption, authentication and access control technologies and services used to carry traffic over the internet" (Balasubramanian et al. 2014), have become so popular with Iranian internet users in recent years. The wide availability of VPNs in the Iranian online market, however, should not be assessed merely from a technological perspective without paying close attention to the socio-political realities of the country. Users may favour VPNs for various technical reasons including their convenience and ease of use, acceptable speeds and even relatively cheap prices. But I argue that VPNs equally serve the regime. Those observers and commentators who see VPNs as an effective response to the regime's censorship policies may need to consider asking why such services are sold legally and often by the very same ISPs that offer filtered connections in the first place.

Paid-for and free VPN and proxy connections are becoming increasingly popular in Iran. In one instance only, American-based non-profit organisation Pillar Fourth Committee (2011) announced that they had started providing one million secure connections to the Internet users in Iran in the first phase of a project which, if successful, could expand to serve a much larger population.

Meanwhile the legality of VPNs remains subject to debate amongst the country's decision-making elite to date. Tabnak (2009), a Persian news website close to moderate conservative Mohsen Rezaie, the former head of IRGC, quotes the seventh amendment of the fifth section of the country's cybercrime law in deeming "distribution of anti-filtering software or of any information which can potentially facilitate neutralisation of the filtering system" as illegal. Gerdab (2010), a website linked to the high-ranking, hard-line security officials operating within FETA and IRGC warns users that bypassing online filters is a crime and that engaging in such activity is punishable by imprisonment (from 91 days to a year) or/and a financial fine ranging from 500,000 to 2 million Tomans (\$200 to \$800). However, Hamshahri Online (2011), another virtual Persian news service published by the office of the currently conservative Mayor of Tehran, questions the authenticity of such claims, arguing that such decisions are usually made by the Committee for Determining Criminal Content, a parallel panel of highly conservative officials, known to be directly responsible for implementing filtering technologies inside the country. The paper quotes Ali Motahari, the head of the Iranian Parliament's Communications Committee explaining that while the law currently forbids using anti-filtering software, VPNs are indeed legal as they are not specifically designed for circumventing online filters and have vital data protection functions for individual users and businesses. Hoghooghddanan (2011), an online society for the Iranian lawyers, also clarifies in an article titled "The Legal Debate over the Use of VPNs" that virtual private networks are perfectly legal to use, according to the current domestic laws.

Justifying VPNs in public adverts by emphasising their security-oriented qualities, rather than their capacity to serve as proxies, not only helps government-run service providers enjoy an increasingly profitable source of income, but also allows them to secretly police and perhaps intercept a huge portion of personal communications otherwise hard to hack. More importantly, the prevalence of VPNs allows the regime to cut off the connectivity of somewhat select users during political turmoil without having to pull the plug on the country's internet altogether. In a highly critical article titled "Governmentalisation of A Civil Affair," Alef (2012), a Persian news website associated with Ahmad Tavakkoi, a non hard-line, Western-educated conservative figure and parliament member, states that "if we suppose that 20 million out of the roughly 34 million Iranian users who regularly access Google and Gmail services inside the country have turned to VPN services following their blockage, and given that these services cost, in average, 30,000 Tomans (just over \$12) per month, a staggering profit of 60 billion Tomans (nearly \$2.5m) must have been generated within only the first two days."

Despite the regime declaring certain uses of VPNs to be illegal outright, the fact that most of these services are subject to identical price tariffs and offer substantially similar technological guarantees makes it hard not to assume a connection between the businesses in question and those ultimately responsible for the filtering technologies applied in the country.

Following the regime's inability to fully justify a criminalisation of VPNs by stretching a certain section of the local cyber laws, the online economic news website Donya-E-Eqtasad (2013a) in July 2013 quoted the former TCI Minister announcing his nationwide plan to

regulate VPNs through monopolisation of the market in favour of the government and thereby ban the private sector from participation. Based on this, the regime would be able both to decide if an individual is eligible to own a secure connection and to regularly monitor this person's traffic to ensure 'legal' usage. Only a month later, however, the same newspaper (2013b) revealed the complete failure of the domestic VPN project, quoting Mahmoud Khosravi, the head of the contracting firm in charge, who confirmed that despite spending billions of Tomans (millions of USDs), only 26 companies applied for their version of VPN.

Policy confusion like this could be a consequence of the Iranian regime suffering from too many parallel decision-making bodies with often inconsistent and sometimes opposing views. For instance, the Persian news web portal Shahrzad News (2012) reported that following the regime's decision to block an array of high profile email services and search engines such as Gmail and Google, many governmental institutions had to take matters in their own hand and equip their staff with the very software deemed illegal in order to be able to continue with everyday duties. This is simply because there are absolutely no domestically developed services that can remotely compare with such sophisticated tools. The BBC Persian service (2013) highlighted this insufficiency by pointing out that Chinese internet users "operate on home grown sites like Weibo, the Twitter equivalent micro-blogging site, and Baidu, a local search engine that is more popular than Google," unlike in technologically dependent dictatorships such as Iran, where citizens rely on foreign services. The article in question also cites Mahmoud Enayat of the Oxford Internet Institute (OII) stating, "there are Iranian equivalents to Facebook, Twitter and YouTube, but none of them has been successful. The likes of Baidu are built by the private sector in China. That can't happen in Iran, as Iranian companies haven't been able to generate an income stream."

Various Iranian cyber-activists based in-country and abroad have regularly reported on changes regarding the development of the filtering system in the country via updates on social networking services, mainly Twitter and Facebook. The micro-blogging website Twitter has been an integral part of almost every major social mobilisation around the world since shortly after its creation in 2006—Iran's Green Movement was among the first globally scalable political movements that embedded the tool in its protests. What distinguished Twitter from many other less successful micro-blogging platforms was, according to Time (2009), that "it's free, highly mobile, very personal and very quick. It's also built to spread, and fast . . . Twitter is promiscuous by nature: tweets go out over two networks, the internet and SMS, the network that cell phones use for text messages, and they can be received and read on practically anything with a screen and a network connection."

The following snapshots of a sympathetic foreign Twitter user's updates calling for hacking attacks to be launched on hard-line websites demonstrate how the service was employed by some non-local cyber-activists to support the Green Movement.

Twitter: Politically Motivated Hacking Attacks Go Viral

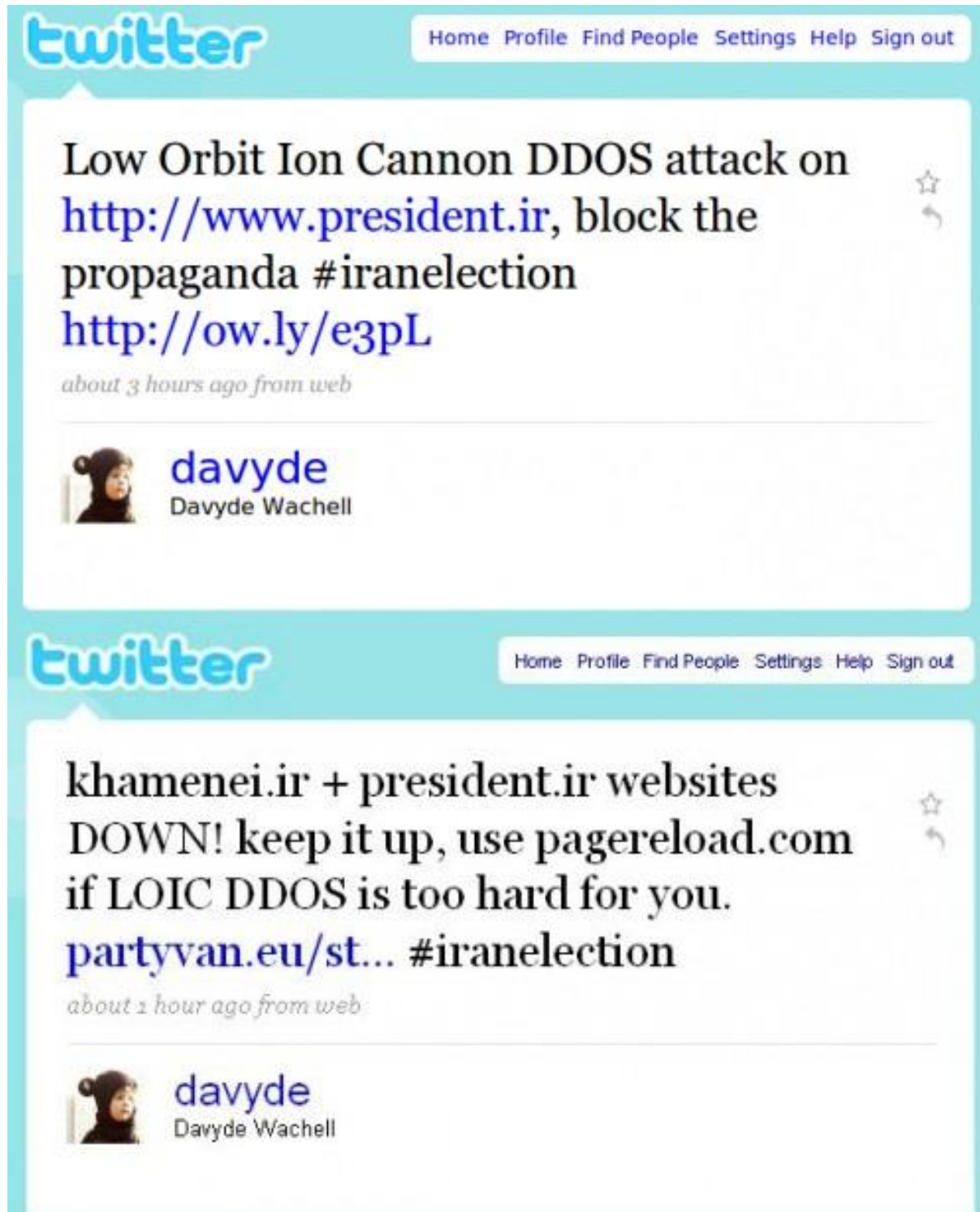


Figure 14 (Twitter 2009, cited by Gadzetomania 2009)

Local cyber-activists in Iran, however, had bigger problems to deal with. The following example shows a familiar 'error message' an Iranian web user tended to face at the time—a government-inflicted outage of online security protocols such as Secure Sockets Layer (SSL):

Google Chrome: SSL Connection Error



Figure 15 (Iran Media Program 2012)

The innovative use of Twitter by Iranian cyber-activists during the 2009 protests presents a particularly noteworthy case, where Twitter offered participants a telephone number to call in order to communicate their Tweets as regular voice messages. These 'alternative' Tweets were recorded onto the Twitter servers and immediately made available as audio files for other users worldwide. This experiment was later developed into a popular service during the 2011 Egyptian uprising, the result of a joint project between Twitter and Google named *Speak2Tweet*. This creative, timely cooperation between two powerful foreign online empires, as Joudeh (2011) argues, simply helped "keep information flowing despite state efforts to shape the public narrative."

Despite a mainstream perception which often reduces expatriate cyber-activists to side-lined observers merely holding up a mirror to events inside their respective countries, there is evidence suggesting that such communities are becoming increasingly independent from their local counterparts, whose reactions to change are no longer necessarily more timely than those based abroad due to various technological advances. A simple example of such independent initiative comes via the following website which helps non-locals determine the latest filtering status of individual URLs within Iran:

Censorship Sniffer: Is 'This' Blocked in Iran?



Figure 16 (Deutsche Welle 2013)

In a feature story titled "Who Is Smarter: Internet Users Or Filtering Officials," the conservative online news outlet Mashregh News (2012) admitted the existence of an innovation-oriented pool of thousands of geographically disconnected local Iranian internet users managing to come up with creative ways to bypass filtering, noting there is almost nothing the government can do to respond in real time. Perhaps that is why online Persian scientific news website Dana Khabar (2013) warns users about a possible nationwide disconnection from all types of VPN. The article explains that VPNs can be easily taken down by disabling a handful of critical tunnelling ports such as Point-to-Point Tunneling Protocol (PPTP), Secure Socket Tunneling Protocol (SSTP) and Layer 2 Tunneling Protocol (L2TP), and points out that the regime may alternatively resort to replacing the internet with a 'purified' national intranet, which might only allow access to a limited number of 'licensed' locally-hosted websites.

It would be extremely difficult to retrieve any meaningful, reliable information on issues such as this directly from the regime due to its closed nature on matters of what it deems as security-oriented data. This may be why about one third of the surveyed experts felt unable to comment on the matter. A majority of the participants, however, believed that conventional, non-VPN, anti-censorship techniques such as TOR and Psiphon are common among and a practical solution for Iranian cyber-activists (Wired 2013).

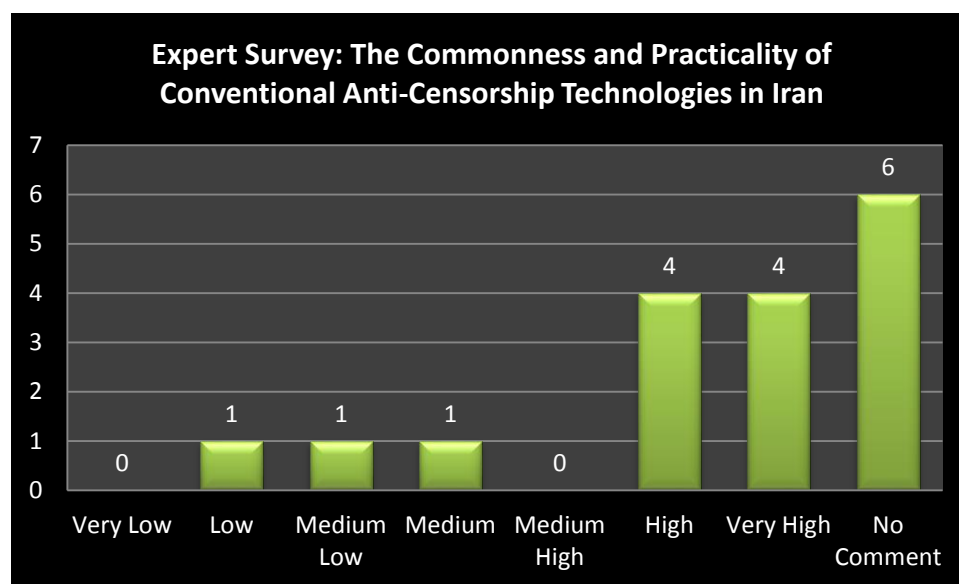


Figure 17

Dr. Babak Rahimi, Associate Professor of Iranian and Islamic Studies at the University of California at San Diego, puts a lot of weight on VPNs as the most effective and widespread anti-censorship solution in Iran due to their effective performance and relatively cheap cost. Neal Ungerleider and Dr. James Fielder are the only other respondents who specifically acknowledged VPNs as a practical anti-censorship solution. The former, however, rejects the idea that they are a 'common' anti-censorship technology, indicating that only a small minority of users have the knowledge and skill to fully and correctly deploy them. Conversely, Dr. Fielder refuses to undermine the social impact of the older 'generation' of online proxy tools such as the TOR network, BitTorrent, CC Proxy, EZ Proxy, Simurgh (seemed to be developed domestically) and other similarly coded software 'solutions'. He, unlike the above two experts, believes that "the only practical and reliable method to evade Iran's censorship regime is through an unblocked proxy server," not the government-regulated VPNs, elaborating that "it becomes a game of cat and mouse between the activists

and the regime, with the activists finding or building new proxies as Iran's Ministry of Communications and Information Technology sniffs them out."

The pattern by which politically motivated technological innovations affect Iran's online sphere may best be explained through Von Neumann and Morgenstern's (1944) Game Theory, also known as Interactive Decision Theory. When applied to the discipline of Political Science, it describes strategic, informed choices made by two or more actors involved in a zero-sum conflict (Myerson 1991). From an IS standpoint, political conflicts are often a particularly prolific environment for technological innovations by all parties involved. As Gregory Asmolov (2012, cited by iRevolution 2012) acknowledges in his study of digital resistance in Russia, "innovations are created by the oppressed, who try to challenge the existing balance of power by using new tools and technologies, but the state can also adapt and adopt some of these technologies to protect the status quo." Perhaps the most outstanding feature of the Asmolov's work is its unique emphasis on the importance of how protesters, rather than necessarily creating new technological tools themselves, innovatively adopt existing new technologies in favour of their cause.

A large portion of the expert participants in this research agree to some extent with Dr. Fielder regarding Iranian cyber-activists' widespread and successful deployment of proxy servers—a testament to the fact that the regime has been largely unsuccessful in its filtering efforts. Also, the active presence of many senior Iranian figures on popular social networking websites such as Facebook and Twitter (Telegraph 2013) proves that the government takes these tools seriously and is aware of their penetration within Iranian society, despite the official ban imposed on them.

Dr. Tessa Houghton, Assistant Professor of Media and Communication at the University of Nottingham, confirms that proxies and other tools of firewall circumvention are the activists' most commonly used technologies, but underlines that these techniques are used not only by this community alone, but also by many other internet users across the country. In her view, "these tools are very practical, and great for promoting solidarity and co-ordination . . . and thus exert pressure for change either indirectly or directly."

Providing individuals with a circuit-based "mechanism of communicating anonymously on the internet" (Thomas and Mohaisen 2014: 173) and initially brought up in Dr. Fielder's interview, the TOR project appeared repeatedly throughout the surveyed experts' answers. Dr. Jed Crandall clarified that he had no credible data on the current state of affairs in Iran, but suggested that those behind TOR were the right people to approach. While none of the experts actively involved in TOR were available to comment on the record, Dr. Marcus Michaelsen, a scholar of Communication Science, claims that Iranians are one of the biggest user groups on TOR—averaging almost 50,000 daily users, including not only activists but also ordinary people seeking to access all kinds of blocked content. He disclosed that "someone from TOR told me that the Iranian authorities are not very successful in discovering connections to the TOR network and that the TOR people were able to quickly counter the few attempts made with deep packet inspection." Dr. Nassim Nazemi, too, has observed that Iranian cyber-activists evade detection and circumvent censorship primarily by routing traffic through proxies and masking their IP addresses. She adds, however, that the reason why these categories of software solutions, led by TOR, are not more popular is that they perform relatively poorly on low-speed networks.

Samples produced by a longitudinal (2008–2010) study of Twitter suggest that Iran is the second largest market for TOR, only after densely populated China (Nawaat 2010). The same study also finds Iranians predominant users of other popular proxy software such as Psiphon and Sesawe. Meanwhile, other democracy advocates have created multifunctional anti-censorship bundles based on existing, open-source technology and aimed not necessarily only at repressive countries. Pirate Browser is a popular example:

PirateBrowser: Open Source Programming at Counter-Censorship Service



Figure 18 (Eddy 2013)

In the same way, LimeWire, a popular, free peer-to-peer online file sharing software promoted itself via an ad-banner campaign during Iran's post-election turmoil encouraging Iranians to defy the regime's censorship by using their software to circulate videos of the protests:

LimeWire: Peer-to-Peer Networking to Fight Online Censorship



Figure 19 (Roettgers 2009)

Yet Limewire was ordered to shut down by a US Federal Court injunction in October 2010, and found liable for causing financial damages to record labels by allowing its users to breach copyright law (Guardian 2010). Such heavy-handed responses to software allowing the free exchange of protected content has caused significant citizen backlash in Western countries,

including the founding of the Pirate Party—a political party first formed in Sweden in 2006 that promotes openness on the internet and now officially operates in 43 countries worldwide. The US governments' war on 'online piracy' has had a negative impact on pro-democracy cyber-activists worldwide. If put into practice, ATandT's latest 'anti-piracy' technology, under which "users [would be] assigned to a so-called risk class, and as a result alleged pirates may have their access to file-sharing sites blocked" (Torrent Freak 2013), could be a crushing blow not only to copyright violators, but also to global political activists who rely on peer-to-peer networking as a method of bypassing online censorship. It will be highly useful, and in fact necessary, to draw a line between legitimate file-sharing and unauthorised reproduction of protected content in order to enhance internet regulations.

Although many types of proxy software are neither produced specifically for nor aimed directly at repressive countries, research conducted by Nawaat (2010) has found evidence proving that "circumvention tools providers and promoters, who claim to address internet filtering globally, have their attention drawn towards almost the same countries." The less democratic a country's ruling structure is, the more it is that the netizens of that country would be inclined to employ online innovations to break communication barriers. Therefore, there will inevitably be a large demand for outside assistance by opposition forces technically unable to match their oppressors' resources.

The Washington Post (2013) deems proxy software employed to circumvent internet filtering to be the most common solution among in-country Iranian cyber-activists, but also observes that regime "authorities have gained the upper hand in recent months, making it difficult to reach many popular websites." On the other hand, Nassim Noroozi, teaching assistant and doctoral candidate at McGill University's Faculty of Education, in a comment left on an Aljazeera (2013) news story, identifies VPNs as the counter-censorship solution most commonly used by Iranian cyber-activists, explaining that this relatively heavy reliance on VPNs means that any serious attempt by the regime to disable certain online tunnelling ports and protocols is likely to create a large information blackout within the country. The BBC (2012) also quotes Mahmood Tajali-Mehr, an Iranian ICT consultant based in Germany, expounding on the alleged popularity of VPNs in Iran as saying that "every schoolchild knows how to bypass restrictions by using VPNs." He never refers to obstacles set up by the regime to hinder the use of VPNs, possibly due to the comparatively older publication date of the article in question.

Various established technology news sources, including Wired (2013), confirm that the Iranian government only officially started tackling VPNs in March 2013. Some other observers report successes, where groups of Iranian cyber-activists have found their way around the regime's VPN blockage. International Business Times (2013) reveals that Project Ainita, an anti-censorship non-profit promoting the use of open source technology, introduced services named 'HTTPS Everywhere' and 'Proxifier' to offer Iranian cyber-activists proxies, encryption and a privacy firewall only days after the new restrictions were put in place. If used together, these would effectively help circumvent the regime's efforts. Similarly, Tech Eye Network (2013) cites Joshua Van Raalte, the owner of a Brazil-based free online proxy software called 'Hide My Ass' as claiming that his Iranian users had remained unaffected by the restrictions. Tech Eye reports that "he thinks that this latest attempt at internet restriction is likely to be largely futile."

The following is one example out of the many web pages run by non-Persian speaking cyber-activists dedicated specifically to offering circumvention of online filtering in Iran:

Foreign Empathy and Internet Censorship in Iran



Figure 20 (Centre for a Democratic Iran 2012)

This research, however, has found no substantial evidence of the aforementioned service ever having been used on a mass scale by Iranian cyber-activists during or after the 2009 protests.

Cyber Police, Online Activists and Self-Reliance in the Virtual Power Struggle in Iran

Home-grown Iranian anti-censorship technologies are almost equally diverse. Yet these tools never became as popular due to factors such as inability to gain users' trust, inconvenience, inconsistent performance, untimely discontinuation, security bugs (Citizen Lab 2012), or permanent elimination by the regime—all problems that seem to be rooted in inadequate funding as well as a lack of technological competence and other vital resources typically needed for time-sensitive, security-oriented projects. To give one example, Access Flickr, an extension for the Firefox internet browser designed to bypass filters imposed on the popular photo sharing website Flickr, was created in the mid-2000s by Hamed Saber. Saber, a local Iranian photo-blogger, was tracked down and arrested (Global Voices 2010) in 2010 for publishing his photos of the post-election street protests:

Access Flickr: Home-Grown Anti-censorship Software in Action



Figure 21 (Global Voices 2007)

Prior to running afoul of the regime, Saber was a male computer hardware engineering graduate, who obtained his degree from Sharif University of Technology (SUT), one of Iran's most prestigious institutions of higher education. He previously attended and graduated from the Allameh Helli High School, an elite school only open to the 'superiorly talented.' In addition, he won a bronze medal at a nationwide IT Olympiad. To give another example, Iran Proxy, known to be the first Iran-based online anti-censorship forum, was founded by cyber-dissident Hossein Ronaghi-Maleki, who has been serving a 15-year prison sentence for his political advocacy since December 2009 (Amnesty International UK 2013).

Sabz (Green) Proxy is an Iranian trace-resistant online proxy software. According to some reports, its technology has been employed by cyber-activists elsewhere (Floss Manuals 2011) to develop anti-censorship systems in their respective countries. Motivated by the regime's drastic enhancement of online censorship following the emergence of the Green Movement in June 2009, the developers kept the software simple, yet highly functional and specifically tailored to the security needs of the typical Iranian user. Further, the programme has been released with a fully Persian-language mode—a first in Iran's history of cyber-activism:

Green Proxy: Breaking through Innovation Barriers



Figure 22 (Floss Manuals 2011)

Simurgh-e-Sabz (Green Phoenix), also simply referred to as Simurgh (Phoenix), is perhaps the best-known 'home-grown' proxy tool developed exclusively for web users in Iran. Once the software is installed on a computer, a user would simply be one click away from bypassing the government's filtering system. This programme, too, was directly inspired by Iran's Green Movement, and has proven to be both popular and effective within the context it was intended for:

Green Phoenix: Endogenous, Functional and Popular



Figure 23 (Citizen Lab 2012)

One of the primary objectives of this research has been to determine the degree of self-sufficiency of both the regime and Iran's cyber-activists in the area of online censorship and to subsequently explain the exact contribution of foreign-sourced ICTs to online power struggles in Iran. While about one third of the surveyed experts had no comment to cast on this particular matter, according to a relative majority of the respondents, as seen in the graphs below, the extent of dependency on imported ICTs was medium to very high at least on the part of the regime and possibly on the cyber-activists' part as well.

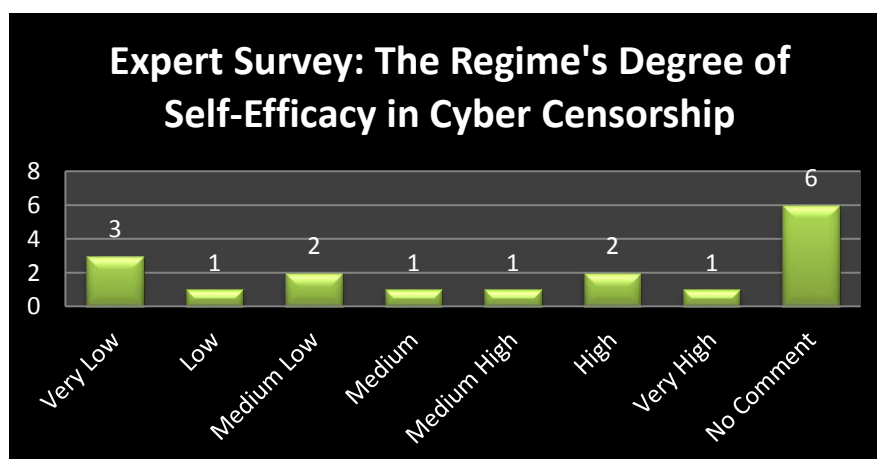


Figure 24

Expert interviews have helped verify the hypothesis that the Iranian regime is largely dependent on foreign ICTs with regards to its online censorship, as Dr. Fielder is the sole respondent to believe that the Iranian regime is largely self-sufficient in this matter. He compares ICT commerce to small arms and aircraft parts and concludes that the state "has access to significant resources and [the] resilience of a mixed economy, in contrast to oil rentier states such as Saudi Arabia." This observation appears to be accurate and consistent with previously published data that identify Iran as the only oil-rich country with the capacity, resources and infrastructure required for a hybrid economy (Muftah 2010).

Dr. Rahimi states that the regime has both borrowed and copied required technology from Nokia-Siemens Networks (NSN) as well as a number of Chinese companies including Huawei. The case against the Chinese firm was fully substantiated via investigative research commissioned by the United States House of Representatives (2012), nearly two years after Nokia voluntarily published (Nokia-Siemens Networks 2010f) a self-assessment report acknowledging there had been a collision between its Western ethical standards and its adherence to local laws in some markets, including Iran.

Despite being accused of the same ethical error, the cases of the above two firms show a significant difference in the Western and Chinese firms' approaches to corporate social responsibility and ethical accountability. It seems that what triggered NSN's official acknowledgment of its evasion of Western standards by engaging in business with the Islamic Republic was a consumer boycott campaign launched by human rights activists in and outside Iran as well as an unsuccessful attempt by a prominent Iranian political dissident to sue the company in US Federal Court. In a democratic environment, a public company has every reason to be afraid of bad publicity and to voluntarily seek to rectify damages it may have caused. Such dynamics played little to no role in the case of Huawei.

The Chinese firm's conduct, on some level, compares to the Iranian regime's sale of weapons to extremist Shiite rebels in neighbouring countries, or to Russia's sale of anti-aircraft missiles to Iran. The bottom line is that most ICT companies, when left to their own devices, might be expected to do business with any paying customer without investigating the nature of the proposed use of technologies sold.

Even if a European firm pulls out of a repressive market for ethical reasons, it will soon be substituted by a Chinese equivalent far less likely to respond to watchdogs' calls to justify some sort of non-adherence to 'Western' values the Chinese firm will claim never to have recognised in the first place. In that light, any future policy will need to take into account the often varying values that govern the ICT industry in different countries and identify and monitor 'high-risk' sellers, making it highly expensive for them to behave in ways that violate international norms.

Elahe Boghrat warns of the regime's natural inclination to convince everyone that they are entirely reliant on in-house scientists and scientific innovations, while "not only the technology, but often the technicians the government speaks of are rented from the West either lawfully or illegally."

Dr. Crandall does not deny that the Iranian government has spurred serious innovations making the best use of the capacities it has, but considers its technological competence to be reasonably low. He considers the regime's attack on the Certificate Authority System to be a huge blow to cyber-activists in Iran, "because the basic level of trust on the internet that

you're really talking to a particular Western company and not to someone in the middle when you use the internet basically fell apart."

Here, he is referring to an episode from July 2011, during which DigiNotar, a Dutch certificate authority, was used to issue fraudulent certificates for Google and to launch a set of man-in-the-middle attacks against the company (Google Online Security 2011). The attacker, though still unknown, was traced back to Iran. Hacking attacks of this sort, which access personal data through faking secure connections between the server and the users while electronically eavesdropping on them, could easily lead to the disclosure of highly sensitive information which the regime can use to identify, arrest and convict thousands of political activists.

Dr. Nazemi finds the regime to be proficient at hiding the inner workings of its domestic surveillance apparatus and quite adept at copying and improving technologies originally developed by others. She adds, however, that this is a "scrappy sort of self-reliance" and that she would be very surprised if the regime was not largely self-sufficient at this point.

Similarly, Dr. Houghton believes that the regime is self-reliant only in terms of on-going maintenance and having the manpower needed to keep its censorship system running, clarifying that it is "heavily dependent upon global TNCs who provide the base infrastructure for such censorship regimes."

Mr. Ungerleider, Mr. Akbarzadeh and Dr. Kluver unanimously agree that the Iranian regime is not very self-reliant in online censorship. Mr. Ungerleider acknowledges that Iran benefits from a large population of coders and IT engineers, but explains that "there are too many structural issues preventing a 100 per cent home-grown internet censorship regime." Conversely, Dr. Kluver asserts that "it [wouldn't] need a tremendous amount to mount a successful surveillance regime."

Expert Interviews: The Self-Efficacy of the Iranian Regime's Current Online Censorship System

Name	Occupation	Location	Expert's Opinion
Akbarzadeh, Pejman	Journalist, Radio Producer and Activist	Amsterdam, The Netherlands	Very Low
Boghrat, Elahe	Journalist, Author and Translator	London, UK	Very Low
Coleman, Kevin	Senior Fellow	PA, USA	N/A (Deems Irrelevant)
Crandall, Jed	Assistant Professor of Computer Science	NM, USA	Medium
Dawoody, Alexander	Assistant Professor of Public Policy	PA, USA	High
Fielder, James	Air Force Major and Holder of a PhD in International Relations and Comparative Politics	TX, USA	High
Hashemi, Layla	Professor of History and Political Science	MD, USA	Very High
Holman, Paul	Professor of Political Science and International Affairs	ME, USA	N/A
Houghton, Tessa	Assistant Professor of Media and Communication	Malaysia Campus	Medium Low
Kluver, Randy	Professor of Communication	TX, USA	Low
Mejias, Ulises	Assistant Professor of Communication Studies	NY, USA	N/A
Michaelsen, Marcus	Holder of a PhD in Communication Science	Germany	N/A
Nazemi, Nassim	Juris Doctor and Law Clerk	IL, USA	Medium High
Rahimi, Babak	Associate Professor of Iranian and Islamic Studies	CA, USA	Medium Low
Storck, Madeline	Holder of an MA in International Relations and Affairs and a MSc in Media and Communications	London, UK	N/A
Ungerleider, Neal	Social Media Consultant and International Technology and Cyber-security Reporter	NY, USA	Very Low
Vahdati-Bana, Soheila	Scholar, Author and Human Rights Activist and Holder of a PhD in Electrical Engineering and Computer Sciences	CA, USA	N/A

Table 5

MIT Technology Review revealed in an online piece published in 2009(a) that while the Iranian regime has a history of relying on software from McAfee called SmartFilter, it has now developed a fully endogenous system which automatically searches for and blocks websites containing certain types of content. It claims Iran and China are the "only two

countries that aggressively filter internet content using their own technology." The journal published another online report (2009b) in the same year, stating that the Iranian government's days of reliance on McAfee technology were indeed over, and that the regime was largely independent from foreign security firms, as almost all of its online traffic "flows through a single government-controlled ISP." Yet, these reports seem chiefly based on speculation rather than on empirical investigation, and are not substantiated with concrete evidence.

Western ICTs vs. Local Politics: European Innovations and the Dynamics of Online Censorship in Iran

This research has found that Western, mainly European; ICT companies have routinely filled the technological hole resulting from the Iranian regime's malfunctioning NIS. While the majority of these firms either deny or legally justify engaging in such transactions, no consistent, reliable data clarify the exact role of Western expertise in systematic censorship in Iran. The expert survey, however, was instrumental in exposing the truth of the matter. Almost half of the respondents thought that European technology played a very large role in the Iranian regime's censorship activities and more than half thought it had at least medium or above influence. About one third of the participants, however, did not feel they were fit to comment on the topic.

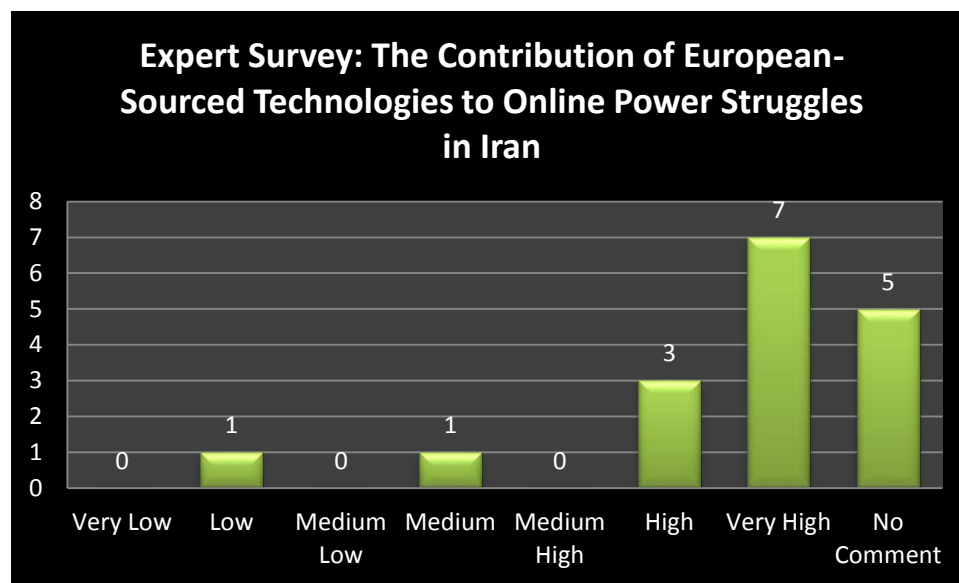


Figure 25

Of all the participants, only one questioned the importance of scrutinising the contribution of European ICT firms to cyber censorship in repressive countries. Dr. Randy Kluver briefly states that he "wouldn't think the European companies [are] that important," since they would simply be replaced by Chinese competitors, if they withdrew from this market.

Many experts mentioned the importance of Nokia-Siemens Networks (NSN). Dr. Alexander Dawoody views NSN's business in Iran as a great damage to the democratic movement in the country, as "the Iranian regime learned from NSN and adapted its technology in creating its own domestic form of TCI." While Dr. Babak Rahmi holds NSN accountable for its role in the aftermath of the 2009 presidential elections, he claims that "since 2010 [the] Iranian surveillance regime has become more domestic-based." Dr. James Fielder and Madeline Storck both verify, on the basis of electronic forensics, that the cell-phone tapping technology

relied by the Iranian regime to arrest many cyber-activists in the aftermath of the 2009 presidential election was indeed provided by NSN, yet at the same time they deny that NSN's presence in the Iranian market was particularly unlawful. Ms. Storck clarifies, "in the Iranian example, the definition of criminal is clearly being stretched." Dr. Jed Crandall, however, suggests that NSN did more than merely provide the Iranian government with interception technology, and that "they reportedly built the system in Tehran used as a chokepoint for the internet, and [which] is critical because it makes man-in-the-middle attacks relatively easy to implement," adding that "few other countries have that kind of capability." Many professional reports, including those published by Reporters Without Borders (2012) and OpenNet Initiative (2013), have confirmed the Iranian regime's use of European technology in launching hacking attacks against political dissidents home and abroad, taking note in particular of technology sourced by NSN and Ericsson.

Other experts refuse to comment on any given company for a variety of reasons, but nevertheless acknowledge the contribution of European-sourced ICTs to cyber censorship in Iran. Mr. Ungerleider stated that as a journalist he was "uncomfortable going on the record without solid evidence of illegal sales of surveillance technology by EU and American firms to the Iranian government or to government-affiliated companies," but nevertheless mentioned that the role of Western companies was "massive." Dr. Tessa Houghton holds transnational corporations such as Cisco and Siemens accountable for their poor attention to corporate social responsibility. On the other hand, Dr. Ulises Mejias puts the main blame on Western governments, asserting that the case of Iran clearly demonstrates that capitalism clashes with any ideals that European or US governments might profess about promoting democracy around the world. He argues "these governments are only slightly less responsible than the corporations, because they have been promoting policies of corporate deregulation that allow the companies to do what they are doing." There are, however, relatively few scholarly sources that deem Western governments more accountable than individual companies for the sale of dual-use technologies to repressive regimes. Although facilitating relevant bottom-up processes within corporate environments to promote good corporate ethics cultures may well prove helpful as a long-term, complementary solution, Western governments cannot afford to ignore policy in favour of self-regulation in an increasingly profit-driven world. Among the various advantages of a policy solution is that it "provides a baseline against which . . . [the firms' performance] can readily be evaluated" (Anand 2005).

A chain of journalistic investigations, triggered by the emergence of Iran's green movement in 2009, and led by news organisations including the BBC (2009a), Bloomberg (2011), Reuters (2012), Wall Street Journal (2011a; 2011b) and the Mail and Guardian (2013) have revealed a number of contracts between foreign ICT firms and the Iranian regime and raised the question of whether such activities are in line with sanctions legislated by the US, EU and UNSC.

The following table shows a list of these foreign firms engaged in ICT trade with Iran, along with the country in which they are based:

Foreign ICTs and Online Censorship in Iran

Company	Location
Nokia-Siemens Networks	Finland
Ericsson	Sweden
MMC Ventures	UK
Creativity Software	UK
AdaptiveMobile Security	Ireland
Trovicor	Germany
Huawei	China
Shenzhen	China
MTN	South Africa
Reach-U	Estonia

Table 6

The above firms' business with the Iranian regime has not been limited merely to 'shelf technology.' Companies have officially agreed to customise, train, and maintain relevant products and have offered other interactive services potentially useful in putting pressure on cyber-activists. This is the case with Nokia-Siemens Networks, whose "sale to and training of Iranian government officials knowingly and wilfully aided and abetted the commission of arbitrary arrest, unlawful detention, torture, and other major human rights abuses" (CBS Interactive 2010).

The pattern detected in the European ICT companies' conduct contrasts with the role that emerges for most of the assessed North-American firms, which have proven to be more dedicated to providing citizens of repressive states with innovative technological solutions to governmental censorship.

North America and the Emergence of Counter-Censorship Technologies

Firm	Software	Location
Censorship Research Centre	Haystack	USA
Ultrareach	UltraSurf	USA
Dynamic Internet Technology	Freigate	USA
The TOR Project	TOR	USA
Citizen Lab at the University of Toronto	Psiphon/ASL19	Canada

Table 7 (Farivar 2011; PBS 2009; Pritchard 2014; Seib 2012)

The findings listed so far form a model which verifies the main hypothesis of this research regarding the bimodality of Iran's NIS and the relationship between imported ICTs and online power struggles in the country.

The relatively rich history of anti-censorship technologies developed in North America, especially in the United States, could be due to the increasing concentration of expatriate Iranians in the region. The presence of such influential lobbyists, many of whom are positioned at the forefront of business or academic worlds, seems to have made a notable impact in terms of convincing and motivating partners to help advocate for freedom of information in Iran and other repressive countries. Perhaps the most significant actor in this regard, the National Iranian-American Council (NIAC) was instrumental in pushing for the passage of the Stand With the Iranian People Act (SWIPA) in the United States House of

Representatives in 2010. The language of the Act includes prohibiting "Federal procurement contracts for companies that provide surveillance and censorship software and other tools of repression to the Iranian government" (NIAC 2010). The mastermind behind SWIPA's introduction was Keith Ellison, Congressman for Minnesota's Fifth Congressional District, who has been extremely vocal about the impact of Western policies on human rights in repressive countries. It is the willingness of the United States Congress to systematically regulate the export of dual-use ICTs to repressive states that has made European telecommunications technology companies into dictators' suppliers of choice.

Iran's NIS, Dual-use ICTs and the EU/US Export Policy Divide

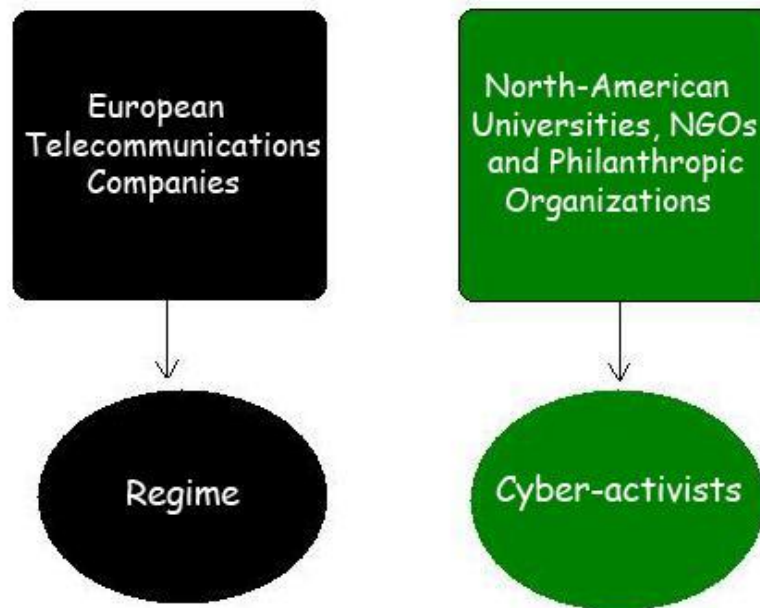


Figure 26

The consistent geographical patterns of imported ICT fuelling either side are directly related to the distribution of the Iranian expatriate community around the world. According to Global Times (2012), an estimated two million Iranians live in the United States and about 500,000 in the United Kingdom, making these two countries the world's top host nations for Iranian expatriates worldwide. The reasons behind the apparent exclusion of UK institutions (perhaps with the exception of the BBC Persian service) from any globally scalable anti-censorship advocacy in Iran, however, should be subject to further research.

The dominant role that the IRGC plays in Iran's mass economy must be added to the above model. Collaboration between military and civilian sectors is not, by any means, unusual or even unconstructive. In fact, as Gummatt and Stein (1997) argue, defence sectors have been instrumental in shaping nationwide innovation processes in many Western countries since World War II. Yet unlike in Iran, where the armed forces and especially the IRGC hold a substantial amount of extra-judicial powers, militaries in industrialised democracies are essentially legitimate and respected sectors of society, dedicated to protecting countries against external threats and to maintaining national security.

IRGC, Nationwide Innovation Processes and the Breakdown of Iran's NIS

In an era of globalisation when conventional physical warfare is becoming less prevalent, Western militaries are increasingly more involved in the production and development of conflict-oriented ICTs. Originally "a spin-off from US military spending" (Financial Times 2011), the internet as we know it today is now a kind of "battleground" of opinions for politically motivated struggles and is, therefore, an influential tool in processes of democratic change. In such an environment, the only way to ensure the functionality of a country's NIS is the establishment of a collaborative and transparent partnership between military and civil sectors, motivating—as well as putting the emphasis on—innovation and development of dual-purpose technologies to address both sectors' legitimate interests and needs. Kulve and Smit (2003) argue that investing in dual-purpose technologies is the best way to maintain an advanced, competitive innovation system based on mutual benefit and trust. They acknowledge, however, that the definition of dual-use is becoming increasingly fraught due to technological advances that raise new ethical issues and in light of innovations that lean towards alarming political goals, such as the Iranian regime's nuclear ambitions:

Technology Development and Intersectional Cooperation: Military vs. Civilian

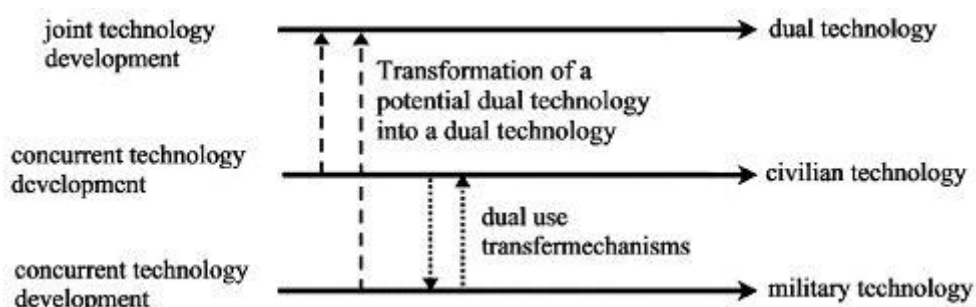


Figure 27 (Kulve and Smit 2003)

In Iran, however, contextual realities tend to guide the country's socio-technical dynamics down a different path than in many other states. If we accept the above model as the basic, functional form of military-civilian collaboration in a reasonably democratic country, the following would best represent the relationship between the two in the Iranian instance:

Technology Imports, IRGC and the Military/Civilian Dynamics of Innovation in Iran

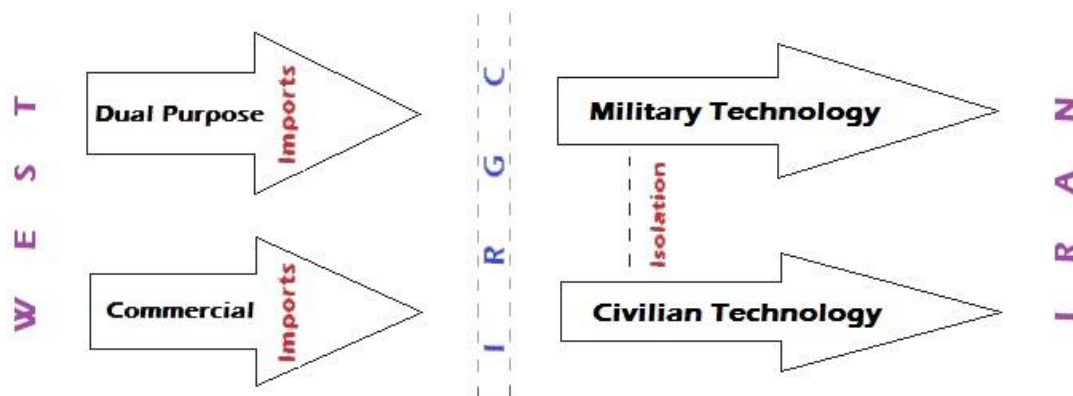


Figure 28

Simultaneously in charge of Iran's economy and military projects, by the end of 2011 the Revolutionary Guards had invested nearly one billion dollars into the development of a cyber-taskforce aimed at boosting its cyber warfare capabilities (Jerusalem Post 2011). This occurred while numerous civilian projects across the nation have been halted or abandoned in the past decade due to lack of funding. This is, as Voelker (2005: 8) notes, far from the 'revolutionary ideals' once promised by Ayatollah Khomeini, the founder of the Islamic Republic, which were mostly civil-oriented. In her assessment, she explains that "the primary concern for Iran is state security and maintaining the region's existing political order." The lack of a reasonable balance between civil and military expenditures by the Iranian regime—a pattern detected in all south Asian countries—has led to what the Royal Danish Defence College (2013: 5) calls 'in-conflict state building.' This phenomenon results in "weak and dysfunctional civilian institutions vis-à-vis stronger and more functional military institutions," the centre reports. With extensive economic sanctions having increased the cost of military-oriented imports to the country, this expenditure gap will only widen in favour of the armed forces, on whose future the regime depends.

About three quarters of the participants remained unable to comment specifically on the role of the IRGC in online censorship in Iran. The remaining quarter, however, unanimously confirmed that the organisation and its allies are heavily engaged in the development of ICTs and various online infrastructures. The interviewees' lack of knowledge about the IRGC and its economic activities could be due to the unusually complicated form of the Iranian state, which has been referred to by observers as a hybrid (Brookings Institution 2013) of a Western-style democracy and a powerful, multi-layered theocracy operating under the Supreme Leader. Under direct command of the Supreme Leader's office, the economic wing of the IRGC dominates almost every business operating at a national scale, often through setting up seemingly private front companies aimed at circumventing international sanctions.

Dr. Alexander Dawoody explains that the IRGC's "contributions [have] strengthened the regime's stronghold on power and caused great damage to democratic mobilisation and town hall-types of cyber meetings." Dr. Babak Rahimi observes a division within the organisation, between civil and military functions, calling for a need to distinguish between the IRGC's private sector and intelligence units within the paramilitary force, arguing "it is the [intelligence units] that [are] in charge of censorship/surveillance infrastructure." Elahe Boghrat says she has discovered that Iran's paramilitary forces, led by the IRGC, "spend billions on complex technological infrastructures to sniff [out] and neutralise online dissent."

Layla Hashemi believes that the Iranian regime is gradually coming to understand the potential of the internet and is exploiting it for core national and international interests, "through the establishment of government funded websites and web logs [and] through censorship of information." Dr. Nassim Nazemi has established a relationship between the IRGC and Iranian universities, explaining that regime has a firm hand in attracting the best and brightest of Iran's remarkably well-educated experts. She claims that "Iran's universities and businesses are just as captive as the average Iranian citizen, and so we have every reason to believe that their best minds are being plundered in furtherance of the regime's censorship and domestic surveillance schemes." All these comments verify the bimodality of Iran's NIS, where defence industries come into conflict with civil innovations in online and offline spheres.

Admittedly unaware of the Iranian context, Dr. Randy Kluver expands on the Chinese model, where GLCs (government linked companies) have had a big role in the configuration of the regime's technological infrastructure. This has allowed "the government to more or less dictate surveillance capacity at a level that was not heard of a dozen years ago." Similarly, Dr. Tessa Houghton recognises government-run companies and universities as extremely critical in repressive states for "providing the regime with a pool of talent from which to draw their cyber troops from [and] to find skilled staff to work on their infrastructure and systems." Yet in certain markets domination by so-called GLCs is not by default synonymous with a malfunction within the respective countries' national economy as can be seen in the case of British Telecom, British Gas, British Airways and British Rail. Instead, I argue, the democratic or undemocratic features of the state are reflected in the functions and dysfunctions of the companies it controls.

In a politically open country, where politicians are true representatives of civilian interest, governmental or public ownership of a company makes little difference to ordinary citizens, as practical, well-enforced regulation aims at preserving transparency within most industries. In a country like Iran, however, there is systematic corruption within the core of the ruling elite (such as IRGC commanders), giving them immunity from accountability. Further, the judicial system is weakened through the existence of parallel institutions controlled by the Supreme Leader and his ideological allies. In this context, nationally owned firms represent much more than mere economic governmentalisation of certain industries. This complex economic power structure underlies the dysfunctions of Iran's NIS. Starosta De Waldemar's (2010: 27) research on the relationship between transparency and resource allocation within an innovation system shows that "corruption and the emergence of new products are strongly correlated." Systematic corruption has an overall negative impact on innovation processes as a general rule. Yet the author's depiction of 'corruption' seems to be mostly focused on the issue of bribing and other matters affecting entrepreneurs operating at the firm level. The corruption rife within Iran's economy is much more thoroughgoing and operates at much larger scales. Iran's economy has been increasingly directly controlled by the IRGC, which Isakow (2011) likens to an "amalgam of the Iranian CIA, Marines, Mafia and Fortune 500." It is now estimated as owning over 30 per cent of the country's businesses. Although independent data are not readily available due to the Islamic Republic's secretive nature, the country's frequent placement at the bottom of Transparency International's (2012) Corruption Perceptions Index should be taken as an indication that the same claim of a pernicious effect of corruption on innovation applies to this national innovation system.

In testimony before the Canadian Parliament's International Human Rights Subcommittee in 2013, human rights advocate Mark Dubowitz explained that the Iranian cyber-police mainly focus "on filtering websites in Iran, monitoring the email and online activity of individuals on a watch list, and observing the content of Internet traffic and information posted on web blogs." The United States Treasury Department's Office of Public Affairs published a factsheet with similar claims in 2012. Yet Mehriran (2010), an online news website based in Germany and published in multiple languages, cites an Iranian official stating that it is the Guidance Ministry and the Telecommunications Company of Iran (TCI) that are the main actors in the regime's internet censorship projects, and that "the IRGC . . . [would only] monitor and be responsible for providing security." Even if that is true, the official in question (or the news agency reporting him for that matter) fails to remind readers that the IRGC owns nearly half of TCI's shares via two of its many front companies, named Mobin Trust Consortium and Sadra and both owned by IRGC's Khatam-al-Anbia Force. They gained control of the heart of the telecommunications industry amid the post-election unrest

in what was the largest transaction in the history of the Tehran Stock Exchange, a combined trade involving 7.8 billion USD (Rooz Online 2010).

Similarly, Jen Psaki, Spokesperson for the United States Department of State revealed in a 2013 statement that "the Iranian Ministry of Communications and Information Technology and the IRGC [had] placed the electronic warfare entity Ofogh Saber in charge of a project to override and spoof commercial satellite communication frequencies emanating from what the Iranian government deemed were subversive Western media sources." While the IRGC has never openly admitted to having any direct presence in Iran's ICT industry, there have been some scattered statements made by the organisation's former and current officials that can be deemed to acknowledge key facts. For instance, Global Information Society Watch (GISW) explains that in 2010 details on the Iranian Cyber Army were not confirmable until Ebrahim Jabbari, the Commander of the Ali Ibn Abi Taleb Ground Forces Regiment of the IRGC, praised the group's achievements in a speech.

One of the many different versions of 'access denied' error messages used by mainstream Iranian ISPs directly mentions the Data Communication Company of Iran (DCI), owned by the IRGC, as the authority responsible for the website blockages:

Access Denied: DCI and Internet Censorship in Iran



Figure 29 (Swift 2003)

The model introduced here should be used to develop policy, as current policies seem to overlook the dynamics of innovation in Iran and in other repressive countries. Unless current deficiencies are addressed, we can expect the continuation of the status quo, wherein foreign

companies make significant contributions to the development of the Iranian regime's telecommunications infrastructure through the sale of 'dual-purpose' technologies produced in democratic countries and wherein civilian and military sectors remained intertwined via corruption and antagonism rather than open collaboration and competition. It is important to differentiate the above phenomena from seldom instances of other repressive regimes knowingly helping their Iranian counterparts either for ideological reasons or in exchange for significant sums of money or other services and favours.

It is conceivable that most European ICT conglomerates develop their ethical codes of conduct statically and based on Western, democratic values, hardly applicable to repressive states where the conceptual borders between criminality and non-adherence to the regime are often obscure. As long as this seems to be the case, we should expect that repressive regimes will easily make up for shortfalls in research and development by signing long-term, exclusive contracts with European Telecommunications firms, openly and legally. Further we can expect that such companies will remain subject to extensive criticism and sometimes even costly boycotts. A lack of adequate, official guidelines, therefore, seems to show that in the international market for telecommunications technologies the concept of Social Corporate Responsibility (SCR) operating alone has proven inefficient.

NSN, a Finnish-German company involved in one of the world's most contested cases of ICT trade between a Western firm and a repressive regime (BBC 2010), has routinely pleaded innocent (Nokia-Siemens Networks 2010a) in response to allegations. The company has announced in various public statements that while they have a commitment to carry on maintaining parts of the country's system under currently valid agreements, they have no desire to expand arrangements with the Iranian regime (Wall Street Journal 2011c). Meanwhile, NSN and various other Western ICT firms continue to do business with the Telecommunication Company of Iran (TCI), now fully owned by the ICG (TeleGeography 2009), either directly through legal channels or via proxies. Yet despite these Western contributions, the speed, coverage and stability of the internet and cell phone networks continue to be among the poorest in the region (Akamai 2013) and the world. This may indicate what parts of the ICT infrastructure are budgeting priorities for the regime and precisely where it is using foreign expertise to fill its widening innovation gaps in its 'security' projects.

By comparison, the private, civilian segment of Iran's innovation system seems to be left facing competition without sufficient resources to succeed. Whereas the hard-line, military-oriented core of the Iranian regime has unrestricted access to 'oil dollars' it needs for acquiring ICTs it is unable to engineer locally, cyber-activists have no other feasible option than to seek out philanthropic 'survival packages' sourced from liberal NGOs and think-tanks worldwide, although there have also been several instances of local Iranian 'innovators,' often with backgrounds in software engineering, positively contributing (PC World 2009) to the cyber-activist community's systematic anti-censorship endeavours. Such individuals, however, have been routinely tracked down and arrested (CNN 2010) by the relatively well-equipped Information Protection (IP) division of the IRGC, accused of 'spreading propaganda' against the Islamic Republic.

The diversity of the interviewed experts' perspective on the research questions poses an analytical conundrum—one that calls for deeper scrutiny. Bearing in mind that the secretive nature of the Iranian administration has been highly influential on the relative inconclusiveness of the interview answers, such degree of variation within a carefully selected group of highly educated scholars somehow raises the suspicion of reason-centred subjectivity. On the other hand, the unexpectedly fluctuating ratio of absolute certainty, together with the relative conviction in which the expressed viewpoints were often emphasised, suggests that the interviewees may have been somewhat opinionated.

This is not a significant finding on its own, given that all the experts were approached as independent informants, as opposed to part of an ideological establishment such as the IRGC. Non-partisan participants in social research can help explain (Li et al. 2015: 201) a "wide range of life experience, interests, knowledge and resources that are foundations for mutual learning, building shared identity and agreement and leading to innovations." They are also highly beneficial to revealing "new or unanticipated behaviours of the system" (Smith et al. 2001: 1). For those reasons, the interviewee population selected by this study was sampled strictly from non-governmental parties, in order to avoid ethical and/or safety complications.

In an attempt to address this issue, the analytical framework for this study has employed a complementary feature known as triangulation, which aims to help determine the credibility of the preliminary findings through multi-methodological examination of the raw data (Shipman 2014).

At the first glance, the main results of this research portray a realistically representational map of cyber-activism in Iran. At the same time, they provide a rich, promising dataset for cross-examination of the online power struggle between the Iranian activists and their opponents within, or supported by, governmental institutions. The outlined disunion amongst the informants can be deemed a demonstration of how the various narratives of a controversial social phenomenon can differ amid a group of disciplinarily diverse, yet equally qualified, scholars. A prime example of this so-called empirical inconclusiveness is seen in the case of IRGC's degree of influence on the development of the internet filtering apparatus in Iran. Given the thoroughness of the conducted background checks on the interviewees, contextual unfamiliarity is highly unlikely in nearly every case.

Validating the Results: A Three-Dimensional Analysis

No.	Research Question	Weblogs	Interviews	Other Published Documents
1	How do actors within the Iranian regime on the one hand and cyber-activists on the other exploit and develop online technologies in their conflicts with one another?			
2	What are the capabilities and functionality of Iran's National Innovation System with regards to telecommunications technologies?			
3	To what extent and why are imported ICTs used in the power struggle between the regime and the cyber-activists in Iran?			

Evidence Strength: Low Medium High Inconclusive

Table 8

Concluding the Research: Hypothesis Revisited

	Weblogs	Interviews	Other Published Documents
Research Hypothesis	✓	X	✓

Substantial Evidence **No Substantial Evidence**

☒ ☐

Table 9

Carefully selected from a preliminary list of potential consultants, the sampled interviewees are all reputable experts in their respective fields. However, the initial scrutiny of the interview scripts pointed to a surprising versatility across the comments and arguments provided by different respondents. This subsequently called for further examination of the participants' depth and scope of first-hand knowledge conducted on an issue-based level.

Dr Alexander Dawoody is possibly the most enthusiastic source interviewed by this research. Answering the questions patiently and at length, he seemed to have a great deal of first-hand knowledge about many of the issues in question, including the Iranian cyber-activists' scope of engagement with ICT innovations, the IRGC's digital censorship strategies and capability,

and the influence of expatriation and gender on the country's online power struggle between the theocratic regime and the pro-democracy opposition. Many of the viewpoints expressed by Dr Dawoody during his interview are also reflected in his 2015 book *'Public Administration and Policy in the Middle East'* published by Springer New York.

Former Oxford Internet Institute visiting fellow researching mainly the implications of ICTs for Shi'a Islam in Iran, Dr Babak Rahimi is the only other Iranian expert on the interviewee list who has published vastly in the field of cyber-innovation. Although he seemed to have a tremendous amount of direct knowledge about the questions at hand, Dr Rahimi chose to be relatively brief, and not as thorough as the research had hoped in terms of technical details. This could have been indeed due to the individual's lack of trust in the interviewer or the nature of the project, as he is known to visit Iran on occasion (i.e. safety cautions). Given that Dr Rahimi is an established authority on both ICTs and modern Iranian politics, his answers, albeit brief, were considered with a highly analytical spectacle.

Elahe Boghrat, veteran London-based journalist and a 2015 nominee for the Courage in Journalism award held annually by Women's Media Foundation, is the only Iranian informant who identifies openly with a monarchist political system as her primary government of choice. Ms Boghrat's responses were perceived as somewhat rebellious in nature, putting her across largely as anti-establishment. She tended to have a good amount of first-hand knowledge on some of the key issues such as the European ICT companies' extent of contribution to online censorship in Iran. As a highly outspoken advocate of atheism and a dedicated feminist, the research speculates that Ms Boghrat's insights on political legitimacy could be characterised in part by an anti-religion bias.

Dr James Fielder was the perfect non-Iranian interviewee for this research. Despite his limited scope of knowledge on some of the specific political issues relevant to post-2009 Iran, he was incredibly open about both his PhD research, as well as about his many-year-long experience as a US Army officer. Dr Fielder made a noteworthy influence on my decision to pursue expatriation patterns as an analytical dimension for the project at hand. Also, he informed the research about Simurgh – an indigenous anti-filtering programme of which I was not aware.

Dr Jed Crandall is an internationally recognised expert in the field of online censorship and surveillance, who specialises in repressive states. In spite of his relatively limited contribution to the research in terms of political depth, he had some invaluable insights about how online innovations may have influenced activism in Iran. Dr Crandal stated humbly on many occasions that his speculations were largely built on media accounts, and that his direct research was restricted mainly to the Chinese context.

A leading cyber-security expert with a distinct focus on politically repressive contexts, Kevin G. Coleman has provided some of the most insightful technical data used at various stages of this research. Mr Coleman has also kept in touch for a considerable while following the interview, forwarding to me frequently the critical updates relevant to my research questions. Coming from a practical background, Mr Coleman believes that the important issue to focus on is not the source of anti-censorship technology, but if and how such tools can be systematically leveraged. Although Mr Coleman demonstrates a relatively great knowledge on the Iranian example, he points to a fundamental void of first-hand data on repressive contexts caused by access and safety issues.

An Iranian expat, politics and history lecturer Layla Hashemi's main contributions to the research fall mainly into the realm of international policy. She is a non-interventionist, believing that modern social movements can only sustain if they are self-reliant in all aspects. However, Ms Hashemi's self-admitted lack of first-hand knowledge on the currently trending anti-censorship activities in Iran makes it challenging to evaluate her comments.

A junior researcher at the time, the answers provided by Madeline Storck were highly instrumental in this study's analysis of the weblog contents. Although Ms Storck stated that her own research had so far remained limited to Egypt, she highlighted two major downsides to most studies of similar nature: a) techno-utopian presuppositions, and b) sampling bias.

I viewed Dr Marcus Michaelsen, former TOR project consultant, mainly as an anti-filtering expert for this research. He demonstrated a considerably high awareness of the local Iranian cyber-activists' circumvention patterns. Dr Michaelsen's comments on internet unblocking technologies and their merits and limitations seemed to be highly credible and based on direct experience.

As a qualified barrister, Dr Nassim Nazemi is the research's sole legal consultant. Her unique insights on surveillance and user anonymity helped open new horizons to topical issues such as trade policy, dual-use technology regulation, and international economic sanctions with regards to Iran's modern politics. An Iranian expat, she makes a clear distinction between the nature of cyber-activism in Iran and in the West, highlighting the dangers of getting exposed in repressive states. Dr Nazemi is the winner of Lowden-Wigmore Prize for Legal Scholarship, and her 2012 paper *'Safe Harbour for Anonymity Networks amid a Cyber-Democratic Storm: Lessons from the 2009 Iranian Uprising'* demonstrates her wide scope of knowledge on the specific matter under investigation.

Neal Ungerlieder's responses were significant to the balance of the research, as his expertise is largely located in investigative journalism. Despite his refusal to comment on certain issues on the record due to his professional commitments, Mr Ungerlieder provided me with many research-based, primary information, emphasising in particular the influencing power of the Iranian diaspora, as well as that of the Western governments and companies in developing what he explicitly refers to as anti-censorship policies. With regards to the Iranian cyber-activists' engagement with online innovations, Mr Ungerlieder acknowledged he had very limited insight into the issue due to being a non-Persian-speaking observer.

During the briefest interview, Professor Paul Holman, who answered only one of the questions in full, humbly declared a lack of sufficient knowledge on most aspects of the subject matter. He, however, underlined the need for a tighter regulation of ICT companies helping out regimes like those in power in Iran, China, Syria and Russia.

A young Iranian expatriate and professional journalist based in Amsterdam, Pejman Akbarzadeh was approached as a voice of Iran's new generation, and the closest interviewee in character to what can be called a grassroots cyber-activist. His ideas revolved around the emphasis on European firms' contribution to online censorship in Iran, as well as on the denial of the IRGC's endogenous censorship capacity. The insights of Mr Akbarzadeh, who is essentially the project's consultant on bottom-up online activism, resonate significantly with those of me as a former political blogger and activist.

An experienced communications educator, Dr Randy Kluver was yet another remarkable influence on shaping the trajectory of this PhD. However, he was somewhat hesitant to engage directly with some of the questions from the outset, underlining the limitation of his knowledge as a distant observer. Dr Kluver kindly offered me to contribute to an anti-censorship project he was associated with at Texas A&M University at the time, which did not end up materialising due to personal commitments.

Dr. Soheila Vahdati-Bana, who is also an expat Iranian author and journalist based in the US, did not agree with the study's premise that there was an on-going online power struggle in Iran. Although she acknowledged the relevance of gender to cyber-activism in general, Dr Vahdati-Bana demonstrated a relatively limited knowledge of issues specific to the context under scrutiny. She came across primarily as a women's rights advocate, and did not engage substantively with any of the 'non-gendered' discussions.

Director of the Centre for the Study of Communications and Culture, Dr Tessa Houghton, is an expert in soft censorship. However, her answers, as acknowledged openly by her during the interview, were based mostly on speculation, and not on any concrete research specific to the Iranian context. Dr Houghton advised me that the European ICT firms' contribution to cyber-censorship in repressive states is indeed a profound one, and that the Iranian regime's (i.e. IRGC) indigenous censorship capabilities are only as good as what they can make of technologies catered to them by large global corporations.

Dr Ulises Mejias contributed to this research largely in an advocational capacity, setting up his responses on a bed of humanitarian principles not necessarily informed by first-hand research or even mainstream media accounts. Firmly in favour of stricter international trade regulations, he underlines the contribution of European ICT companies to censorship in Iran, China, Egypt, and Libya. Dr Mejias came across as a devout socialism advocate. "Capitalism trumps any ideals that European or US governments might profess to have about promoting democracy in the world," he stated, boldly likening NSN's cooperation with the Iranian regime to that of IBM with Nazi Germany during WWII.

All the above consultants were offered an initial set of standard information about the study, in advance of their participation. According to Seidman (2013: 50), when it comes to the protection of the interviewees from adverse future impacts of speaking openly on sensitive issues, the "prevailing principle must be equity". This is so long as reasonable measures are taken by the researcher to ensure that the interviewee has been fully briefed about the intended purpose of the research and its likely socio-political consequences for their careers, as well as providing them with a fair and transparent chance to withdraw statements or request modifications to them at any time prior to publication. The research at hand acknowledges based on previous experience the significance of interviewee protection, even though it did not generally tend to encounter any major examples of potential endangerment. This is possibly owed to my constant attempts to find a middle ground in each case that mutually served the study's objectives and the participant's interests and rights. In Rizk's (2003: 981) view, the core ethical principles of social research might require the researcher to eliminate some "exciting material" from their publication, or even to "slightly distort the results" if they face a dilemma as to which side to prioritise. The researcher, on that basis, will ultimately have no legitimate choice but to "trade-off between the accuracy and punch of [their] report", he argues.

Incidents of such nature were a rarity during the course of this research, as all the participants were selected warily from already outspoken figures in their respective fields of expertise. Oddly enough, there were multiple instances where the interviewees expressed grave concerns regarding the safety of my family members back in Iran, indicating that they were very well-informed about the political dynamics within the country. There were only a few brief moments along some interviews when the interviewee abstained from responding to a question altogether for a reason other than the self-confessed lack of sufficient knowledge. None of those reasons were directly or indirectly entrenched in a fear of the Iranian regime.

The most memorable of those instances occurred when interviewing Mr. Neal Ungerleider, who quite disappointingly refused to engage with my question on Nokia-Siemens Networks (the fourth question on the list), stating that he "felt uncomfortable" as a professional journalist to "go on the record without solid evidence of illegal sales of surveillance technology by EU and American firms to the Iranian government or to government-affiliated companies." He on the other hand referred me to the "impeccable research" conducted on the matter by Privacy International, which according to him "spoke for itself", further indicating the reliance of many industry experts on a handful of reportorial (although often highly accredited) media and NGO accounts. Nevertheless, the strategy used to craft the design of these semi-structured interviews could have been enriched in hindsight by way of discussing explicitly with each interviewee the possible implications of speaking on the record on distinct issues such as specific acts of Western companies or governments in the past. 'Would have it been better practice to persuade the participant to reconsider their decision in return for a guarantee to mask their true identity in the thesis?' is also a methodological doubt that has echoed through my mind looking back at the research results. But then again, one wonders if the hypothetical addition of minute extra bits based possibly on speculation would have been worth compromising the credibility of the thesis by resorting to pseudonyms.

As traditionally common in most non-positivist qualitative enquiries (Galland et al. 2010: 2), there are often more than one, and possibly even conflicting, answers which may stem from "disagreement, outdated information or simple errors." Referred to by Ishizuka and Matsuda (1990: 77) as a deductive interference mechanism, the intended logic here is one which openly recognises the significance of incomplete facts, including "hypothetical knowledge, knowledge with exceptions, and common sense knowledge."

The key challenge here seems to be the recognition of a need for, as well as contribution to the development of, an innovative mechanism which is capable of theorising research results in a consistently accurate and meaningful method. Such a framework, as Parameswaran and Polyzotis (2011: 3) observe, can involve either "majority voting – have several human workers tackle the same question and then take the most frequent answer – [, . . . or employing] a more elaborate scheme where potentially conflicting answers are assigned probabilities, and [where] correct answers are defined based on a probability threshold."

In order for a research design to produce candid results throughout, the most significant factor will have to be the thorough reliability of the collected data. Gammelgård et al. (2007) count four main elements they suggest every qualitative social investigation based on first-hand participatory (i.e. semi-structured interviews) data should note: source proximity, age of answer, area of expertise, and years of experience. But having full control over all these sensitive variables is a rare occurrence in social research, and a privilege seldom enjoyed by activism researchers in particular. The sampling process based on which this thesis was designed has put the focal emphasis on the latter two factors, acknowledging the practical limitations it endured with regards to implementing the other two.

A relatively common technique often employed to validate the research results in non-positivist research areas is triangulation, which essentially involves the study of various sources' perspectives on a given phenomenon (Hussein 2009; Mathison 1988), as well as attempting to make sense of the emerging patterns and trends within the process. However, the often overlooked angle regarding the notion of triangulation in Social Sciences is that the technique is "not aimed merely at validation but at deepening and widening one's understanding" Olsen (2004: 1). This will indeed help set the focus of academia on broad learning processes, and not on trivial inter-disciplinary commotions. The international community will benefit vastly from shifting its rather fixed understanding of triangulation to a more dynamic standpoint or, as Moran-Ellis et al. (2006: 5) assert, an "epistemological claim" focused largely on the maximisation of what can be learnt from a scholarly enquiry.

Seale (1999: 472), too, underlines the primarily educational function of the concept, arguing that the common misrepresentation of analytical triangulation in Social Sciences has been encouraged by researchers "who mistakenly believe in inevitable logical connections between paradigm positions and techniques."

Despite occasional overlaps, triangulation in social research should not be automatically translated into a mere methodological diversity. Alternatively, the concept could involve "comparing interview data from several witnesses to an event, [. . . or] comparing observational data from various settings that bear on the same knowledge claim" Hammersley (2008: 23). Triangulation needs to acknowledge the occasional inconsistencies in the incoming data feed or, as Fielding (2012: 125) states, reflect the crucial understanding that "one cannot measure precisely the same thing twice, [and that] validating an analysis by replication is misguided," due to the essentially fluid nature of sociological processes.

A significance of the constructivist school of thought is, in part, owed to its capability to simultaneously recognise and work with various parallel conceptual narratives which might exist surrounding a given social phenomenon. Under such conditions, methodological triangulation is not necessarily just aimed at "assisting the researcher [with] the research question" (Golafshani 2003: 604).

The notion of triangulation has been widely undermined within the wider scholarly community. In fact, research validation techniques are not particularly popular amongst some less senior social scientists. A possible reason why triangulation is considered by many academics as unconstructive, according to Guion et al. (2011: 3), is that it "can be time-consuming . . . , [as well as requiring] resources that are not always available to lead researchers." Nevertheless, most qualitative researchers' criticism of triangulation remains (Hammersley 2008: 32) to revolve around "a negative reaction to . . . technicism, [and] an insistence on the interpretative judgment necessarily involved in the research process."

Despite such claims, this thesis has found the practice to be beyond just a data validation technique, and highly beneficial to the development of one's understanding of the research topic, as well as to the self-reflexivity process.

Reflexivity, or as Breuer and Roth (2003: 188) describe it, the "recognition of cultural blind spots" in qualitative investigations, is a constructive approach through which the rhetorical "assumptions and values of social scientists may be uncovered" (May 1999). Although retrospective attempts at the discovery of circumstantial limits to previously tested data collection methods "may seem a gloomy affair" (Jensen et al. 2003: 176) at first glance, they often result in the production of considerably more accurate results than otherwise would have been possible to achieve.

Cyber-Activism, Network Literacy and the Innovation of Change

Innovation-oriented levels of computer-literacy are crucial to all online social movements. In the case of Iran in the aftermath of the 2009 unrest, as Washington Times (2009b) reports, hacktivists "were active in helping keep channels open as the regime blocked them and [in spreading] the word about functioning proxy portals," acting as well to take down "Mr Ahmadinejad's website in an act of cyber-disobedience." Nic Newman (2009) of Reuters Institute for the Study of Journalism at Oxford University, observed very little balance in the depth of activism between the pro-democracy activists and regime-backed netizens, as measured on major social networks such as Twitter, explaining that the "conversation was overwhelmingly in favour of opposition candidate Mir Hossein Mousavi, who tended to attract the support of younger, more computer-literate Iranians," including those in the West. NBC (2013) reports that Iran benefits from a large population of young, highly educated and web-literate citizens, who can potentially make the country a leading power in cyber-activism. "Names and web addresses of proxy server sites that allow users to sidestep controls are passed around like hot gossip," the agency informs. International Relations Review (2013) argues that regardless of the regime's vigorousness in online censorship, the "computer-literate generation is able to circumvent these obstacles."

Data collected from the sampled blogs enable us to conduct a methodical assessment of some of the most politically active Iranian cyber-activists:

Persian Bloggers, Computer Literacy and Innovative Use of Online Technologies

Item No.	Blog's Name	Blogger's Degree of Computer Literacy	Evidence of Innovative Use of Online Technologies
1	Political Humour	Intermediate	No
2	Political Humour: Jokes About Ahmadinejad and Khamenei	Advanced	Yes
3	Arman Dekami	Intermediate	No
4	Alireza Rezaee	Intermediate	No
5	Green Iran Forever	Advanced	No
6	Short Messages	Intermediate	No
7	Gameron	Advanced	No
8	Mr. Asghar	Advanced	Yes
9	F. M. Sokhan	Advanced	No
10	Sayed Ebrahim Nabavi	Advanced	No
11	Nikahang Kowsar	Advanced	No

12	Eghbal Mahoori	Intermediate	No
13	Mullah Piaz	Intermediate	No
14	Mehran	Intermediate	No
15	Darush Ariaee	Advanced	Yes
16	Mana Neyestani	Advanced	No
17	Maatine	Advanced	Yes
18	Rain in the Half-opened Mouth	Advanced	Yes
19	In Between	Intermediate	No
20	What Kind of Country Is This?/What Is Up Today?	Beginner	No
21	Our Future	Advanced	No
22	Takhhand	Intermediate	No
23	Today's Front Pages of Newspapers	Intermediate	No
24	Mr. Khosn in Exile	Advanced	Yes
25	Prophet Yarou	Beginner	No
26	Facetious Sayings	Advanced	No
27	Samovar	Advanced	No
28	Anti-dictator	Beginner	No
29	Zekipedia	Beginner	No
30	Brainless Money	Advanced	Yes
31	Talented Moron	Intermediate	No
32	Anger Flame/Shadow of Freedom/Democratorship	Intermediate	No
33	Sight	Intermediate	No
34	Of Cowardice	Advanced	No
35	Serious Humour	Intermediate	No
36	Amjadiyeh	Intermediate	No
37	Basiji Jokes	Intermediate	No
38	Dambooli	Intermediate	No
39	Iran's Green Revolution	Advanced	No
40	Iran Got Ruined	Intermediate	No
41	Dude	Intermediate	No
42	Green Man	Intermediate	No
43	Vision Is the Truth	Advanced	No
44	Green Alliance	Advanced	No
45	Green Movement: We Are Countless	Advanced	No
46	Qom's Green Movement	Advanced	Yes
47	Green Musings	Advanced	Yes
48	Senaps	Intermediate	No
49	Balagari	Advanced	No
50	Hollywood	Advanced	Yes
51	Mir Ali Sabzineh	Advanced	No
52	Mullah Hassani	Advanced	No
53	Khan Gor's Musings	Intermediate	No
54	Land of Iran	Intermediate	No
55	Moghilan Tree's Thorn	Advanced	No
56	Other Side of the World	Advanced	No
57	World of Humour	Advanced	No
58	Uncle Changiz	Advanced	Yes

59	Rebellious	Advanced	Yes
60	Annamaz	Advance	No
61	Hidden Sense	Intermediate	No
62	Sober, the Little Prophet	Advanced	No
63	Iran Lover	Advanced	No
64	Superstition and Broken Clock Hands	Advanced	No
65	Dried Whey	Advanced	No

Table 10

An analysis of the above indicators leads the research to the following results:

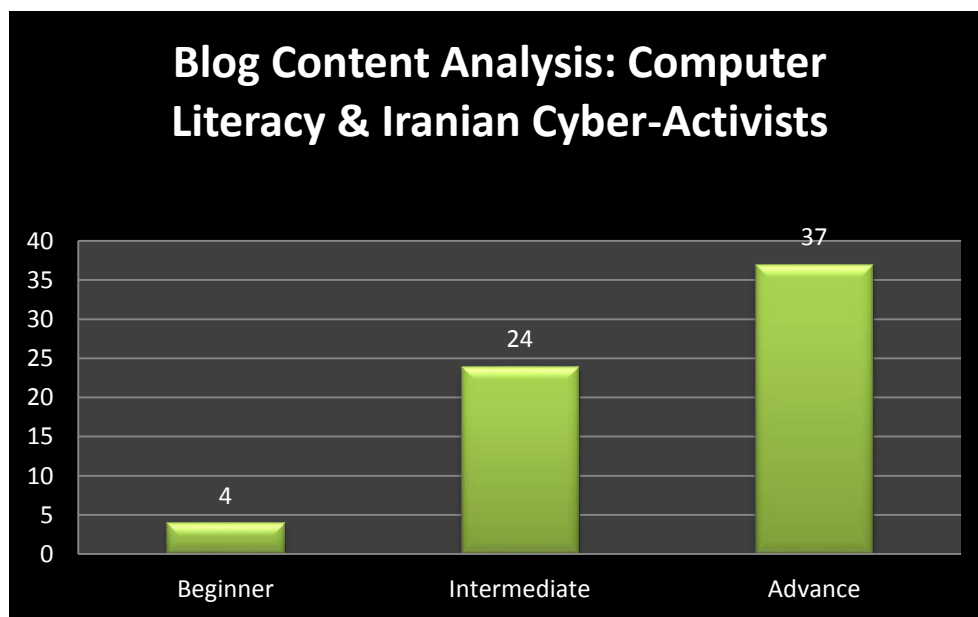


Figure 30

The relatively high rates of computer literacy among politically motivated Iranian cyber-activists tend not to coincide with any high degree of innovativeness within the opposition movement. It remains largely consumption-oriented—53 out of the 65 bloggers made little or no original contribution to the development of anti-censorship software. This inconsistency is particularly worthy of analysis, as the dysfunctions of the Iranian CIS are not likely to be symptoms of a shortage of relevant expertise, as this country boasts some of the most prestigious Science and Technology research centres in the Middle East.

Recognising the difference between computer literacy and actively engaging in innovation is crucial to understanding and explaining the current status of Iranian cyber-activists within the country's NIS. In 2009, Iran ranked first in the world for its growth rate in science and technology—development in these areas being eleven times faster than the world's average. It ranked seventeenth in terms of the production of computer science applications (Science Metrix 2010), while topping the World Internet Stats' (2012) table of internet usage in the Middle East with nearly 42 million connected citizens, translating into just over fifty-three per cent of the total populace. But if Iranians' computer literacy is so high, why are the nation's netizens and cyber-activists not especially prolific in producing online innovations?

It seems that computer literacy rates may not have as much relevance to the generation of timely, practical online innovations as some might expect. This may partially answer Hasse's

(2011) question regarding "the relation between practice-based learning, technological literacy and innovation." The aim here is not to discount the significance of education, but to underline the effects of resource deprivation on the civil half of Iran's NIS. It would be impossible, even for the nation's brightest software developers, to out-innovate foreign systems backed technologically by industry giants and funded to the tune of billions of USD, especially without any meaningful financial input. That would compare to going into a real war with a plastic gun. When young experts find themselves unable to beat the system, they will have only two economically viable options—either to migrate abroad as skilled workers, or to serve the regime's oppressing forces directly or indirectly by eventually seeking work within a governmentally-directed industry. Most people in this predicament will fall into the second category for contextual reasons.

The circle of innovation at the national level in Iran is defective when compared with the model for democratic countries as developed by Lundvall, where academia, governmental institutions and enterprises collaborate in a unimodal system towards one single, transparent end. This dysfunctional NIS has led to what is often referred to as an innovation chasm: a lack of constructive and logical coordination between universities and industry to address the society's legitimate needs—as opposed to secretive, ideological goals—due to the absence of democracy within the political framework. Russell (1953: 49) argues that in contest between a democratic country and a repressive one, "the one allowing liberty is almost certain to become superior to the other in war technique in no very long time." This claim has been substantiated empirically in the case of Iran, whose online (Atlantic Council 2013) and offline (Elleman 2013) offensive powers remain below the standards of many Western states, despite having spent nearly \$6.3 billion (SIPRI 2013) on its military in 2012.

In a news article published during the post-election turmoil in 2009, Wired (2009) reported that at the same time as the demonstrators were gathering on the streets of Tehran and other major cities, their local and expatriate online equivalents were organising and launching hacking attacks on various governmental websites. "In both Iran and abroad, the cyber strikes are being praised as a way to hit back against a regime that so blatantly engaged in voter fraud," the magazine reported. Although it is generally believed that these hacking attacks were at least partially conducted by ordinary Iranian cyber-activists, as opposed to professional, paid hacking groups, there is also evidence to suggest that the Green Movement received a great deal of technical help from sympathetic professionals at home and abroad. In one instance, Radio Free Europe/Radio Liberty (2011) detected ties between anti-regime cyber strikes and the prominent hacking group Anonymous. RFE/RL quotes an Iranian member of Anonymous named Arash who was briefly interviewed over the phone. Acknowledging their online facilitation of the DDoS attacks in question, he states: "We know how powerful Iran's Islamic regime is, and we know it is hard fighting against them. But we have hope. And we are lucky because we are fighting on the side of the people of Iran."

Mapping the Geography of Cyber-Activism in Iran: Counter-Censorship Innovations and the Local/Expatriate Divide

This research also links the geographical location of Iranian cyber-activists to their degree of innovation and their exact contributions to power struggles with the ruling elite. Expatriate Iranian pro-democracy cyber-activists bring a different dimension into play. Indymedia (2010) describes Iranian expatriates residing in the US as "uberly educated"—a phenomenon that seems to largely apply to Iranians based in north-western Europe as well. This could be due to their unrestricted access to information and the often much improved access to

academic education. Iran's expatriates tend to be more in touch with the contextual realities of their country of origin than many locals tend to perceive. Uskowi (2013) reported shortly after the June 2013 presidential election that about half of the expatriate community voted for the sole non-conservative candidate available to them—Hassan Rouhani—a proportion fully consistent with his share of the polls inside the country, where he achieved about fifty-one per cent of the vote. One possible conclusion here is that the Iranian expatriates were heavily affected by the negative consequences of the regime's hostile foreign policy during the eight years of Ahmadinejad's presidency, and therefore felt an urge to support the anti-extremism campaign launched by Rouhani and his moderate allies within the inner circles of the Islamic Republic.

Estimated to number in the tens of thousands, cyber-activists associated with this segment of Iran's political discourse are responsible for an array of anti-censorship activities ranging from fundraising to developing proxy software to engaging in DDoS hacking attacks. Yet expatriate software developers have not been immune from prosecution by the cyber police (HRANA 2013; Near East Observatory 2013). Longitudinal (2009–2011) content analysis of sixty-five popular politically active Persian blogs, reformist and secular, sampling equally from those based inside and outside of Iran shows that expatriate Iranian cyber-activists may not be more concentrated in the United States than in other Western countries. This finding is not in line with previously published data (Naghdi 2010) mapping the Iranian diaspora suggesting that nearly forty per cent of expatriate Iranians are based in the United States. Alternatively, this distribution could be an indication that Iranians residing in the United States are less politically active and/or computer literate than their counterparts elsewhere, despite their larger population. The rest of the assessed bloggers tend to be scattered worldwide, primarily in north-western European countries, where most international human rights NGOs are headquartered. For twenty-two bloggers, a geographical location remains fully unknown, while two of the expatriate blogs contain no explicit evidence of the country from which they are maintained:

Persian Bloggers: The Geography of Online Dissent

Number	Blog's Name	Blog's Address	Blogger's Location
1	Political Humour	http://tanze30ya30.blogfa.com	Unknown
2	Political Humour: Jokes About Ahmadinejad and Khamenei	http://ba27.wordpress.com	Unknown
3	Arman Dekami	http://g791.wordpress.com	Iran
4	Alireza Rezaee	http://alirezarezaee1.blogspot.com	France
5	Green Iran Forever	http://greeniranforever.blogspot.com	Toronto, Canada
6	Short Messages	http://tweatter.blogspot.com	Iran
7	Gameron	http://gameron.wordpress.com	Bandar Abbas, Iran
8	Mr. Asghar	http://www.asgharagha.com	London, UK
9	F. M. Sokhan	http://www.fmsokhan.com	Iran
10	Seyed Ebrahim Nabavi	http://www.enabavi.com	Belgium
11	Nikahang Kowsar	http://nikahang.blogspot.com	Toronto, Canada

12	Eghbal Mahoori	http://www.khodnevis.org/persian/author/eghbaly	Unknown
13	Mullah Piaz	http://mullahpiaz.net	Unknown
14	Mehran	http://www.khodnevis.org/persian/author/mehrancartoonist	Unknown
15	Darush Ariaee	http://sansornashode.blogspot.com and http://persiaroyal.blogspot.com	Unknown
16	Mana Neyestani	http://zamaaneh.com/zamtoon/cat	Malaysia
17	Maatine	http://maatine.com	Iran
18	Rain in the Half-opened Mouth	http://www.debsh.com	Malaysia
19	In Between	http://andarmal.wordpress.com	Unknown
20	What Kind of Country Is This?/What Is Up Today?	http://mamlekate.blogspot.com and http://emroozchekhabar.blogspot.com	Unknown
21	Our Future	http://ayandema.blogspot.com	Christ Church, New Zealand
22	Tahkhand	http://tahkhand.blogspot.com	Iran
23	Today's Front Pages of Newspapers	http://safhehaval.blogspot.com and http://sepehr1970.blogspot.com	Unknown
24	Mr. Khosn in Exile	http://blog.hasanagha.org	Oslo, Norway
25	Prophet Yarou	http://yaarou.wordpress.com	Unknown
26	Facetious Sayings	http://www.hazl.com	California, USA
27	Samovar	http://samavar.wordpress.com	Expatriate, Location Unknown
28	Anti-dictator	http://zobin-cost.blogspot.com	Unknown
29	Zekipedia	http://zekipedia.wordpress.com	Isfahan, Iran
30	Brainless Money	http://brain-less.blogspot.com	LA, USA
31	Talented Moron	http://talentedmoron.blogspot.com	Unknown
32	Anger Flame/Shadow of Freedom/Democratorship	http://anger-flame.blogspot.com , http://freedom-sayeh.blogspot.com and http://democrator.blogspot.com	Unknown
33	Sight	http://tanzir-balatarin.blogspot.com	Unknown
34	Of Cowardice	http://bozdelaneh.blogspot.com	Unknown
35	Serious Humour	http://werraj.wordpress.com	Iran
36	Amjadiyeh	http://amjadiyeh1900.blogspot.com	Iran
37	Basiji Jokes	http://basijoks1.wordpress.com	Unknown
38	Dambooli	http://dambooli.wordpress.com	Tehran, Iran
39	Iran's Green Revolution	http://irangreenrevolution.wordpress.com	Iran
40	Iran Got Ruined	http://hamid.thepersianland.com	Unknown
41	Dude	http://melisagodwin.blogspot.com	USA
42	Green Man	http://sabzemard.wordpress.com	Unknown
43	Vision Is the Truth	http://visionisthetruth2.wordpress.com	Tehran, Iran
44	Green Alliance	http://ettehadesabz.wordpress.com	Tehran, Iran
45	Green Movement: We Are Countless	http://nehzatsabz5.blogspot.com	Tehran, Iran

46	Qom's Green Movement	http://greenqom.wordpress.com	Qom, Iran
47	Green Musings	http://worldqress.wordpress.com	Iran
48	Senaps	http://senaps.blogspot.com	Iran
49	Balagari	http://balagari.wordpress.com	Tehran, Iran
50	Hollywood	http://hollywoodweblog.wordpress.com	Shiraz, Iran
51	Mir Ali Sabzineh	http://miralisabzineh3.wordpress.com	Tehran, Iran
52	Mullah Hassani	http://mollah.blogspot.com	Toronto, Canada
53	Khan Gor's Musings	http://khangor.blogspot.com and http://khangor.blogfa.com	Mazandaran, Iran
54	Land of Iran	http://persiatazmin.wordpress.com	Unknown
55	Moghilan Tree's Thorn	http://naiem.wordpress.com	Australia
56	Other Side of the World	http://onvaredonya.blogspot.com	Copenhagen, Denmark
57	World of Humour	http://hosseinpooya.blogspot.com	London, UK
58	Uncle Changiz	http://www.bipfa.com/amoo-changiz	Unknown
59	Rebellious	http://fetnegar01.blogspot.com	Unknown
60	Annamaz	http://annamaz.blogspot.com	Iran
61	Hidden Sense	http://chinejan.wordpress.com	Iran
62	Sober, the Little Prophet	http://marooned9.blogfa.com	Iran
63	Iran Lover	http://ashegiran.blogspot.com	Unknown
64	Superstition and Broken Clock Hands	http://khorafe.blogspot.com and http://mehdiyaghoubi38.blogspot.com	Expatriate, Location Unknown
65	Dried Whey	http://kashkmyblog.wordpress.com	Iran

Table 11

Based on the above, the geographical distribution of the sampled bloggers can be condensed into the following chart:

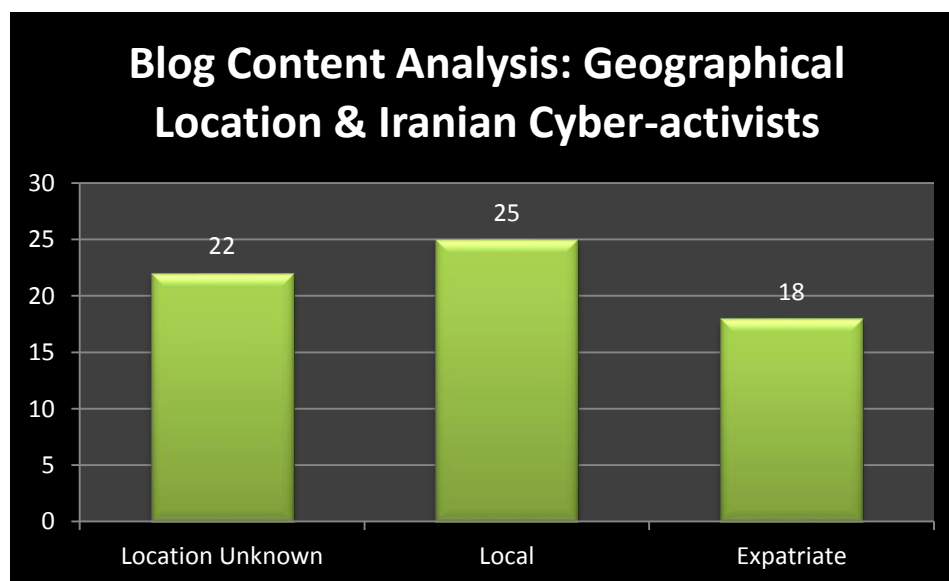


Figure 31

A mapping exercise conducted on the eighteen assessed expatriate blogs reveals the individual countries in which their owners are based:



Figure 32

The results show that the Persian blogs sampled are nearly equally divided between North America, Europe and the rest of the world in terms of the location from which they are maintained. This suggests that Iran's top expatriate cyber-activists are mostly based in Canada, the United States and north-western Europe. There is a direct relationship between the migration pattern of the Iranian political exiles and political openness of their countries of settlement. It appears that most dissidents who leave Iran are inclined to settle in countries where they expect to be able to make the greatest impact on their homeland's future.

In fact, a major contributor to the dysfunctions of the Iranian NIS is brain drain, or as the Wall Street Journal (2009) refers to it, a "spreading refugee exodus of businesspeople, dissidents, college students, journalists, athletes and other elite Iranians that is transforming the global face of Iran's resistance movement." Iran suffers from one of the world's largest brain drain effects (Daily Reveille 2013). If we accept that the majority of 'ground-breaking' technological innovations in a given country are made by a superiorly talented, highly educated young elite, then it cannot be deemed as promising for the country's NIS that Iran faces an annual loss of between 150,000 and 180,000 of its academic specialists, costing the country nearly fifty billion USD (BBC 2007). Currently, there are 250,000 Iranian scientists permanently residing only in the United States or Canada (BBC Persian 2011). Another 50,000 Iranians are registered higher education candidates studying abroad (Iranian Embassy in Norway 2011), including many who will refuse to return home following graduation due to a lack of job security (New America Media 2011), and to an extensive restriction of social freedoms (Pars Times 2000).

In the expert interviews, opinions on the influence of geographical location on the innovation activities of Iranian cyber-activists were highly polarised. Elahe Boghrat has very little doubt that expatriate Iranian dissidents have been more successful in such activities. This is "due to liberal nature of the Western countries where most of them reside," she explains. In full agreement with the above statement, Dr. James Fielder believes that the role of expatriate cyber-activists in the development of anti-censorship technology remains largely underexplored, and says that he can see this conceptual gap even in his own doctoral dissertation, explaining that "the link[s] between urban locals and expats are more crucial than links between urban and rural locals. A vigorous information pipeline depends on not only a robust network but also educated and savvy users."

Layla Hashemi, however, disagrees, stating that she believes "the call for political change should and must come from within the nation." Dr. Marcus Michaelson fully acknowledges the contributions made by expatriate cyber-activists, but says he has heard from reliable sources that "Iranian activists from inside the country are very capable of finding ways to counter filtering and censorship." He, nevertheless, raises the question of whether the country's local activists have the technological capacity and infrastructure to do this efficiently. Dr. Nassim Nazemi also believes that despite their relatively smaller numbers local Iranian cyber-activists' "actions have a greater immediate impact on the regime," adding, "expats have a less important role to play." Finally, Pejman Akbarzadeh, journalist and producer at the Amsterdam-based Persian language radio station Radio Zamaneh, asserts that local activists' "views on the situation can be more realistic because they are inside the country."

Based on the results of this research, expatriate Iranians are considerably more capable of engaging in 'conflict-friendly' technological innovations, which could be due to a range of factors including access to specialist educational opportunities on all levels, open political systems, and infrastructure with far superior connectivity when compared to their counterparts residing in Iran. A large proportion of Iranian university students enrolled abroad, especially those studying at the post-graduate level, are engaged in hard science programmes. If such courses of competitive quality were run inside the country, this would not likely be the case. In terms of its average internet speed (2.53 Mbps), Iran ranks (Net Index 2013) 163 out of 186 countries surveyed, preceded by Tunisia (2.55 Mbps) and followed by Lebanon (2.46 Mbps). Adding in Iran's position as the least free state on Freedom House's (2013a) Net Freedom list—beating China and Cuba by a few points—it becomes clear why academia has increasingly failed to address the true professional aims and aspirations of the country's top computer science students, who often either get banned from working in the field or emigrate shortly after graduation. This subsequently creates a void of expertise in the local market, making ICT imports even more vital to Iran.

The Iranian ICT industry remains, for the most part, technologically hostage to the Islamic Republic's security-oriented policies. According to a report published by Freedom House (2013b), the TCI Ministry issued a directive addressed to all the ISPs, "asking . . . [them] . . . to separate internet traffic from intranet traffic, in line with the continued implementation of the National Information Network (NIN)." This would speed up access to 'approved,' locally hosted websites, while still keeping access to unfiltered websites hosted by non-Iranian servers painfully slow, making them awfully difficult to browse. Perhaps it is hoped that this clever technical trick will boost the country's currently very low position on the Net Index, allowing the authorities to escape some of the international pressure they face for their extensive violation of internet rights.

Other experts refuse to grant technological leverage to any one group of cyber-activists based on their geographical location, and emphasise the differences between the two communities rather than the superiority of either's influence. Madeline Storck further elaborates on this perspective, explaining that "local cyber-activists played an important role in planning and organising protests, while expatriate cyber-activists' role was more in generating awareness in the wider world of the events taking place within the country in question." Dr. Ulises Mejias views the expatriate activists' actions as facilitating local ones, saying that the "expatriate community is mostly responsible for disseminating information about the movement, and [for ensuring] that the use of social media by local cyber-activists is limited but focused and effective." These two comments help confirm the existence of a single collaborative network

of interconnected Persian cyber-activists dedicated to pro-democracy dissent in place within the online sphere. If extensive filtering, vigorous surveillance and low speed connections were effective at preventing local Iranians from connecting to the 'outside world,' this would have been clearly reflected in interaction between cyber-activists based inside and outside the country. But the current structure of the internet—Web 2.0—seems conceptually too dynamic to get trapped by set, inflexible frameworks. Local and expatriate cyber-activists have shown over the years that there is very little that oppressive forces can do to limit their potent partnership. But the mere existence of a golden opportunity for innovation does not necessarily translate into a timely, efficient 'strike.' The evident reliance of local Iranian netizens on foreign ICTs seems to have restricted the output of a CIS that could otherwise be considerably more prolific.

The Internet and Democracy Blog (2008) claims that its original content analysis of a selection of Persian blogs demonstrates that the "blogosphere [in question] is a . . . communication space where a wide variety of political, literary and artistic themes are discussed by Iranian expats and a broad cross-section of those living in Iran." The BBC (2009b) refers to the Iranian blogosphere as "a well-connected [network of] expats, experts and academics." American Thinker (2013) observes that at the height of Iran's latest presidential election the expatriates played a key role in "reporting that the revolutionary guards and the religious police are out in force, watching as citizens vote—ostensibly to make sure they vote for the 'right' guy." Aljazeera (2009), acknowledges the Iranian expatriates' role during the post-election unrest, quoting prominent blogger Potkin Azarmehr stating in an interview that "given how internet savvy the young Iranians are and the help they are getting from Iranian expats, whatever law Ahmadinejad passes, there will be a way round it." The Toronto Star (2013) dedicated an article to Ali Bangi and Mahsa Alimardani, two Iranian-Canadian internet security experts who designed ASL19 at the University of Toronto's Citizen Lab. "ASL19 facilitates internet access for people in Iran, where access is tightly controlled," the paper reports. Working closely with other major anti-censorship software developers, including those behind Psiphon, they warned (ASL19 2013) local Iranians in June 2013 about an allegedly fake version of the program rapidly circulating on the web, posting tips on how to distinguish it from the genuine file.

Explaining innovation dynamics in Iran—a country divided against itself—calls for various adjustments to the traditional conception of NIS. Iranian expatriates have been integral to the pro-democracy movement (Aljazeera 2012b). Mostly computer-literate, politically active and based in industrialised democracies, Iranian expatriates have influenced online power struggles in several ways. They have developed and/or promoted anti-censorship software, organised boycotts against Western telecommunications firms that continue to do business with the Iranian regime, harassed pro-regime websites with DDoS attacks, and persuaded Western politicians and NGOs to systematically support the free flow of information in Iran. Some of these expatriates have been involved in the development of some of the world's most effective proxy software. Other members of the Iranian expatriate community are known to have been influential in improving the relevant databases needed for better functionality of such software, given their direct knowledge of the contextual realities of the target market. In terms of shaping international policies, the most prominent example is the Washington DC-based National Iranian-American Council (NIAC), a non-profit that claims to have been lobbying for the improvement of human rights in Iran since its formation in 2002, and pushed for the Iranian Digital Empowerment and Stand with the People of Iran Acts at the United States Congress in December 2009.

Network Access, Computer Literacy and Online Innovations: Gender Equality as a Catalyst of Change

Although the feminist movement has a rich history of engaging with pioneering technological innovations (Chen and Xiao 2011; Wajcman 2013), techno-feminism remains to be viewed by many (e.g. Puleo 2012; Rowbotham 2013) as one-dimensional and partisan. Nevertheless, the core significance of modern feminism lies chiefly in its keen focus on the social elements influencing technological trajectory at all stages of the innovation, adaptation and use.

Classic feminism traditionally regards technology as gender blind, criticising mainly the patriarchy issue for women's unjustifiable exclusion from hard sciences. Techno-feminism, on the other hand, has a tendency to embrace social constructivism, simultaneously ruling out absolute neutrality and un-negotiable technical bias of the scientific innovations. This progressive approach has been imperative to the modern-day feminists in their breakthrough of some social barriers, and in helping them move along (Faulkner 2001: 92) toward "a practice that is more democratic and respectful of diversity." This particularly resonates in the field of ICTs, where "higher proportions of males than female [are] reporting access" (Selwyn 2004: 344). The requirement for the embedment of feminist philosophy within the theoretical construction of this thesis stems fundamentally from gender consciousness (Bierema 2003). Although many male sociologists across the globe have the most progressive of intentions in mind with regards to gender equality, some of their research approaches may be driven unknowingly by socially accepted patriarchal concepts and forces (La Pastina 2006).

The interplay between gender and ICTs is not merely of a historical or technical nature, but is also a product of the social conditions in which those technologies are adapted and used, or as Wajcman (2009: 7) refers to, a "seamless web or network combining artefacts, people, organisations and cultural meanings and knowledge." Therefore, understanding that the initial design of a given hardware or software does not necessarily determine the trajectory of its possible future transformations is imperative to the feminist techno-science research.

The compulsory exclusion and voluntary abstinence of the female workforce from actively participating in the ICT-mediated industries is deeply interwoven with the contextual realities of the offline world, namely the patriarchal nature of the multinational corporate businesses (Menon 2015; Phillips 2014). As a result, the question of computer literacy becomes less of a relevant factor than the immediate need for attention to the women's struggle to choose between their social image and entering uncomfortable territories, or as Wajcman (2007: 289) puts it, "forsake their femininity" in favour of short-sighted economic gains.

The techno-feminism approach to online innovations argues that no amount of pre-release technical tests can produce assurance in terms of future gender popularity or usefulness, and that a functional innovation system necessitates a "mutual adjustment of technologies and gender identities" (Oudshoorn et al. 2004: 13) over the long term.

Gender, Democratic Legitimacy and Innovation: A Sociological Approach to Cyber-Activism in Iran

Gender is another factor neglected by the conventional conception of NIS. Northern European nations are widely recognised as pioneers of gender equality, and arguably the world's freest countries for women to live in.

The following comparison of the Gender Inequality Index (GII) rankings in 2008 and 2011 simply shows that the top 10 (out of 138 and 146 respectively) positions are almost entirely shared between the same countries, all of which (with the exception of Singapore) are located in the north and west of Europe. Moreover, the table demonstrates that countries with lower gender inequality in 2011 have also topped the same year's Human Development Index (HDI) ranking list:

Gender Inequality Index: 2008 vs. 2011

Country	GII Ranking 2011	GII Value 2011	HDI Ranking 2011	GII Ranking 2008	GII Value 2008
Sweden	1	0.049	10	3	0.212
Netherlands	2	0.052	3	1	0.174
Denmark	3	0.060	16	2	0.209
Switzerland	4	0.067	11	4	0.228
Finland	5	0.075	22	8	0.248
Norway	6	0.075	1	5	0.234
Germany	7	0.085	9	7	0.240
Singapore	8	0.086	26	10	0.255
Iceland	9	0.099	14	13	0.279
France	10	0.106	20	11	0.260

Table 12 (United Nations Development Programme 2011)

Such gender-neutrality, as D. Chen (2004: 3) suggests, is "an essential component of an effective economic and human development strategy." It is helpful to note that all these countries are among the most economically developed. But is gender equality a pre-requisite for economic success or is it the other way around? The above researcher quotes the World Bank (2003) as stating that "development policies and actions that fail to take gender inequality into account and fail to address disparities between males and females will have limited effectiveness and serious cost implications." This may help explain why Iran consistently ranks poorly in regards to both the gender gap and economic development.

Gender inequality is not, as some may perceive, merely an issue of ethics and social justice. By systematically discriminating against women in academia and/or the workplace, a society deprives itself of roughly half its potential resources and expertise. Gender discrimination directly disrupts all elements of an NIS in its classic (i.e. Northern European) sense, and prevents any given national system of political economy from fully flourishing, regardless of fiscal investment. The world's increasing focus on gender equality "is a central component of the process of democratisation," as Inglehart et al. (2002: 21) argue. Without democracy, as previously argued, a country's NIS becomes tainted with negative surprises. The democratic nature of an NIS, therefore, can be considered a measure of its overall, long-term capability, functionality and sustainability—offering yet another reason why Iran is, on many levels, dependent on foreign technology.

The country's consistently poor position on the Global Gender Gap (GGG) ranking list is a testament to this claim:

Global Gender Gap Report 2009

Nation	GGG Ranking	Population
Pakistan	132	176,242,949
Saudi Arabia	130	28,686,633
Iran	128	66,429,284
Egypt	126	83,082,869
Turkey	129	76,805,524
Qatar	125	833,285
Yemen	134	23,822,783
Mali	127	12,666,987
Chad	133	10,329,208
Morocco	124	34,859,364

Table 13 (World Economic Forum 2009)

Meanwhile and in contrast to the north-western European states discussed above, Iran's HDI ranking remains just above average in the world and across the region:

Human Development Index 2011

HDI Ranking	Country	Score
17	Israel	0.888
30	UAE	0.846
37	Qatar	0.831
42	Bahrain	0.806
56	Saudi Arabia	0.770
63	Kuwait	0.760
64	Libya	0.760
71	Lebanon	0.739
88	Iran	0.707
89	Oman	0.705
92	Turkey	0.699
94	Tunisia	0.698
95	Jordan	0.698
96	Algeria	0.698
113	Egypt	0.644
119	Syria	0.632
130	Morocco	0.582
132	Iraq	0.573
154	Yemen	0.462

Table 14 (United Nations Development Programme 2011)

Another outcome of this research worthy of reflection is the striking imbalance of the distribution of the interviewees in terms of gender. Although selected from a larger directory of carefully sampled online journalists, cyber-activists, and scholars of activism and computer and political science, a quick glimpse at both lists is enough to show that most—if not all—of these areas of expertise are dominated by males.

This phenomenon brings to mind the question of the relationship between politically motivated cyber-activism and gender, on which there happens to be no scholarly data. Psychological research (Eagly and Steffen 1986), however, shows that there is a direct relationship between gender and aggressiveness, demonstrating that males are both physically and socially more confrontational. This may help explain male domination of conflict-oriented fields.

While the role of gender equality on a country's economic development may be relatively easy to establish, there seems to be an escalating need for a coherent explanation for the relationship between the two and technological innovations, and further for a robust framework to address NIS inadequacy in repressive countries such as Iran. Reaching the bar set by largely innovation-focused north-western European economic powers seems to be a reasonable plan for these states. Danilda and Granat Thorslund (2011: 20) quote a paper published by Central Europe (2010), a European Union programme which encourages cooperation among nine central European countries, as stating that the "equal participation of men and women is essential . . . to exploit the full potential of innovative strengths—not only for demographic reasons, but also in case of innovation processes and results." They call for new policies that can effectively re-balance gender representation in innovation processes of business and research in favour of the professional female workforce.

Andersson et al. (2009, cited by Danilda and Granat Thorslund 2011: 29) also emphasise the role of gender equality in economic development, claiming that "a more open working climate and a broader approach to developing products and services boosts the competitiveness of the individual organisations and the regional innovative environment." But the question still remains: how can the West rectify the situation through policy? Questioning repressive regimes on their discriminatory gender laws, such as Iran's ban on female enrolment in various university programmes, would be a promising start. Archibugi (2004: 181) argues that, at least in the case of the United States, we are facing a blatantly 'schizophrenic' approach to issues such as gender discrimination, asserting that "It is US national policy to consider as anti-social, if not criminal . . . using gender-discriminating nouns. Yet such quibbles are soon forgotten when US policies assume a foreign dimension."

A central part of this research, the results of a longitudinal (2009–2012) study of sixty-five politically active Persian blogs equally divided between locals and expatriates show that only one blog was maintained by a woman. This suggests that despite common perceptions holding the regime's ideology of male preference to be solely responsible for damaging the professional aspirations of Iranian women, even the stratum of society most devoted to change seems to suffer from the same degree of gender inequality, ultimately making it equally undemocratic in nature.

Over one third of the surveyed experts acknowledged gender as an influential factor in cyber-activism in the Iranian context, but very few had firm opinions or access to any recent, solid data on the issue. Dr. Alexander Dawoody insists that Iranian women, especially those educated in the West, have taken the lead and are in the forefront of the cyber-activist movement in Iran. According to him, they are "experts in finding ways to offset regime offenses through modest, yet determine[d] and continually developing technological solutions to TCI." Dr. Dawoody, however, does not substantiate this claim with any concrete evidence. Dr. Soheila Vahdati-Bana, a human rights advocate and expert in Electrical Engineering and Computer Sciences, claims that "women with children find it more convenient to connect with others via the web," yet also fails to provide evidence. While the latter claim falls

slightly outside of this research's zone of focus, the former does not correspond with data retrieved through blog content analysis, which suggest that women are heavily underrepresented in the country's cyber-activist community. There seems to be a growing need for empirical data on the participation of and attitudes of Iranian women towards cyber-activism—a valuable resource from which this research could have greatly benefited.

Dr. James Fielder claims that cyber-activism is a practice shared almost equally between Iranian men and women, as long as we are assessing urban areas. He suggests that "greater conservatism and fewer educational opportunities create larger gender cleavages [outside of major cities]." Yet this argument is not quite consistent with the results of the blog content analysis, which demonstrate a gender gap. Although the exact geographical locations of the sampled in-country Persian blogs remain undetermined in most cases, it would not be unreasonable to assume that they are run mostly from bigger cities. This is because in Iran the chance of having access to a broadband network connection, as well as the skills required to purposefully employ it to create content, rises sharply with the size of the city. Also, the majority of the competent Iranian universities are based in the country's most crowded provinces.

A PBS (2008) report acknowledges the widespread presence of Iranian female activists on the internet and their engagement in a range of innovative activities, ranging from creating and circulating radio podcasts to disseminating information through expanding email lists. The report alleges that "for the first time, the women's movement is not restricted to a certain elite, but includes women of all ages and backgrounds, from big cities to small villages." The Women's UN Report Network (2010) cites Parvin Ardalan, prominent Iranian women's rights activist and winner of the Olof Palme Prize in 2007, stating in an exclusive phone interview that "every print magazine for women we had was closed, so we created a new world for ourselves in cyberspace."

Similarly, CNN (2013) quotes Barbara Miller, winner of Amnesty International and WACC-SIGNIS Human Rights Awards for her documentary about three international female cyber-activists in exile (including an Iranian one), as saying that "a refusal to be censored unites . . . women across cultures and continents, as they use their blogs to connect with the world outside of the regime." The BBC (2002) seems to have a slightly different take on what motivates Iranian women to get online, arguing that "the web is providing a way for women in Iran to talk freely about taboo subjects such as sex and boyfriends." It also anonymously quotes a 'leading' female Iranian cyber-activist who explains: "I could talk very freely and very frankly about things I could never talk about in any other place, about subjects that are banned." While this information may not necessarily be accurate over a decade later, it may help explain why women are so under-represented in Iran's cyber-activism scene, despite their reportedly large presence online.

Male dominance in the Iranian community of politically motivated cyber-activism does not coincide with advanced IT skills or ground-breaking anti-censorship innovations. The egregious gender gap within Iran's cyber-activist community is not, as some may assume, an outcome of discrimination in the country's higher education system, but instead the result of biases enforced at all levels of a conventionally male-dominated society. Evidence shows that, with the exception of only a few fields reliant on heavy labour, such as mining, auto-mechanics and aerospace engineering, about seventy per cent (Masoud 2006) of graduates from engineering university programmes are women. Yet the fact that over half of the country's skilled forces have very little chance of contributing to their country's technological

development, in comparison to their—not necessarily more qualified—male counterparts, provides a reasonable explanation for Iran's distorted innovation structure.

D. Chen (2004: 3) asserts that "there is a statistically significant positive association between gender equality in education and economic development," emphasising the positive influence of ICTs on both. Klasen (2002) spots a reciprocal pattern in his research, arguing that gender bias in education disrupts economic development by limiting human capital, which in return affects literacy. Yadav (2006: 2) explains that the "movement towards gender equality is not a technocratic goal—it is a political process. It requires a new way of thinking in which the stereotyping of women and men gives way to a new philosophy that regards all people, irrespective of gender, as essential agents of change."

This insight is quite important for the idea of a 'genderless' innovation system as proposed by this research. Despite the popular perception that all debates regarding gender equality are psychological in nature, it is argued here that religiously and culturally motivated gender discrimination in Iran has had a noticeable impact on nationwide innovation processes. In other words, a lack of democratic features such as gender equality will most likely result in the distortion of a country's NIS.

A content analysis of the Persian blogs sampled by this research demonstrates that a dominant ninety-four per cent (61 out of 65) of the bloggers were male, whereas only one of them was certainly a woman, while gender remained unknown for three of the bloggers:

Persian Bloggers: Gender and Cyber-activism in Iran

Number	Blog's Name	Blogger's Gender
1	Political Humour	Unknown
2	Mullah Piaz	Unknown
3	What Kind of Country Is This?/What is Up Today?	Unknown
4	Khan Gor's Musings	Female

Table 15

The disproportionate gender distribution of top Iranian cyber-activists is in blatant contrast with previous studies of the country's university graduates, especially those obtaining science and engineering degrees. Iranian women currently constitute about seventy per cent (LA Times 2012; Masoud 2006) of the 'hard' science and engineering university students nationwide—making Iran one of the world's top states in terms of female expertise. Suffering from an even more severe degree of workplace patriarchy, Al-Zahra, the IRGC's only all-female unit (Taheri 2007), had no more than 400 'qualified' recruits (Cordesman 2007) by the end of year 2003.

Women and Higher Education: A Worldwide Comparison

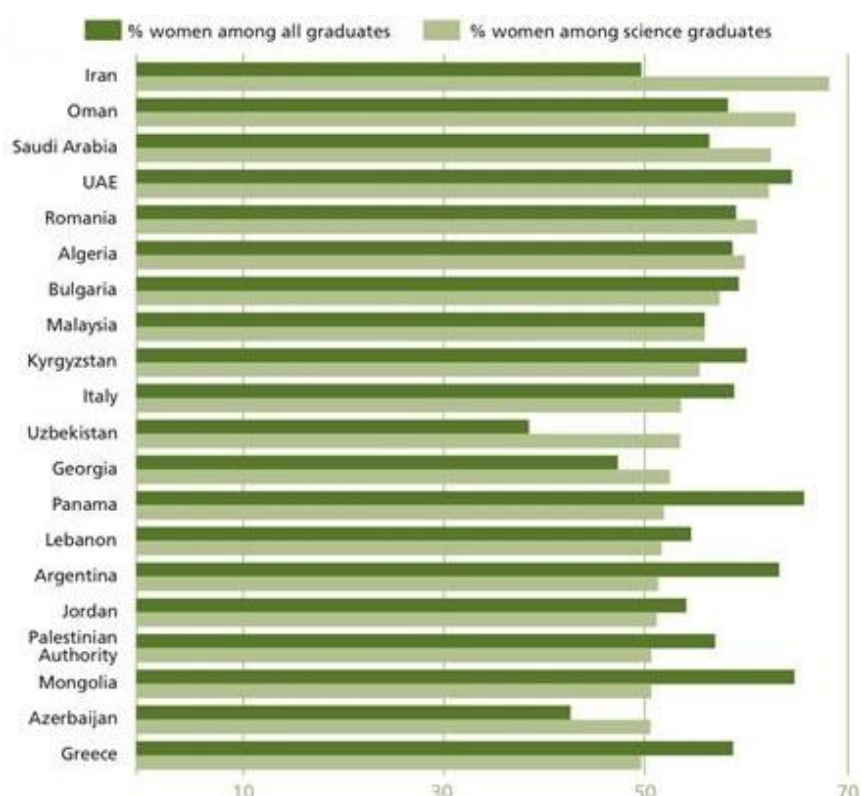


Figure 33 (UNESCO Data Centre 2010, Cited by Charles 2011)

An empirical comparison between the number of Iran's female degree-holders and female representation in the professional workforce across all branches of hard science, along with the country's official position as the world's top nation in terms of female graduates in science and engineering programmes, leads to the conclusion that the Iranian NIS has a large and unnatural void of female experts—a practical obstacle not addressed by Freeman and Lundvall's original conception of NIS. When such a large percentage of potential experts are effectively barred from participating in developing new innovations, the resulting NIS cannot be truly functional. Although an extremely valuable contribution to the Innovations Studies literature globally, the existing NIS model tends to view nationwide innovation processes from a democratic, gender-neutral perspective—yielding a framework only relevant to a limited number of Western, industrialised nations. Such a 'clinical' model is not adequate for a country like Iran that has profound issues of gender inequality. Structural alterations will need to be made to the existing model for it to become fully applicable in this context.

The lack of gender equality in either mode of Iran's NIS is not rooted in academia. Despite cultural limitations, Iran remains a world leader in terms of its number of female university graduates, outpacing an array of economically more developed countries. What makes Iran a poor guardian of women's rights, however, is a deeper, contextual issue. While many bright, professional Iranian women have complained about professional discrimination, statistically they also appear not to be integral in the 'alternative' political sphere, where participation is based more on voluntary engagement. This cannot be solely due to a state-inflicted lack of opportunities, instead reflecting the contextual realities, including the vulnerable place of Iranian women in virtually all of the country's discourse as an 'intellectually inferior' gender. This stereotype is commonplace, despite standing against (Woolley and Malone 2011) every concrete piece of evidence gathered to date.

Iranian women online therefore face additional roadblocks to participating in an efficient CIS. They not only encounter cultural obstacles to effective representation, but must also navigate the same technical impediments faced by all Iranian netizens. Iran has been a regular member of the world's least free internet access club for many consecutive years:

Iran's Internet Freedom Status (0 = Most Free, 100 = Least Free)

	2011	2012
Access Restriction	21	21
Content Control	29	32
Individual Surveillance	39	37
Total Score	89	90

Table 16 (Freedom House 2012)

All Iranian cyber-activists will benefit from well-researched and effectively promoted policies, led by the democratic world, that emphasise gender equality and the development of anti-censorship technologies while consistently denying the Islamic regime's access to dual-use ICTs.

Legislative Powers of the European Parliament: Policy as a Preventative Measure

A great majority of the surveyed experts acknowledge the need for policy solutions to these issues, recognising that Western legislators, including the European Parliament, are among the most potentially powerful actors and have the ability to shift the pattern of online censorship in repressive countries in favour of local pro-democracy forces.

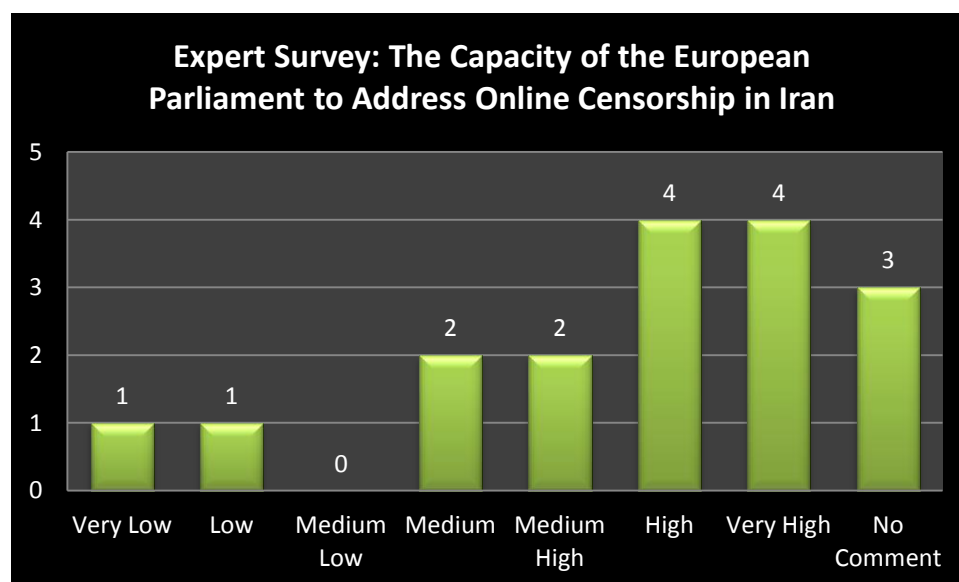


Figure 34

In his interview, Dr. Alexander Dawoody called for new laws to be adapted in four broad areas:

- **Penalising** companies such as NSN who do business with tyrannical regimes and support the suppression of opposition movements or any form of expression.
- **Rewarding** innovations and companies that clearly support democratic aspirations, human rights and ethics in business.
- **Funding** research aimed to further develop ICTs as a viable tool in civic mobility and civic action, through loans, grants, and donations.
- **Boycotting**, criminalising, and sanctioning all business, research, and technologies associated with regimes that censor citizens and enforce tyrannical forms of governance against the will of its people.

Similarly, Dr. Babak Rahimi sees an urgent need for international laws "prohibiting the sale and intelligence sharing of any computer-related technology that could be used for surveillance purposes." Elahe Boghrat explains that individual governments or the EU cannot currently really force any company to refrain from business with a repressive regime like the Iranian one. She suggests, however, that targeted sanctions would be an effective solution, as they would simply force corporations "to abide by the rules or else . . . face the consequences." She claims that "the embedment of ICT-related knowledge and equipment into these sanctions can cause the regime many big troubles." Dr. James Fielder suggests as well that, once sanctions are placed, evading companies should be held accountable for contracts made with repressive regimes. He strongly challenges the argument that the European Parliament does not hold much power in the grand scheme of things, arguing that "While the European Parliament may lack direct coercive authority, it can apply incredible political influence that ultimately pressures states to toe policy lines."

Dr. Nassim Nazemi says she cannot overemphasise the importance of sanctions, as the Iranian regime is highly dependent on technological imports. She believes that sanctions are "an efficient way to cripple this regime," while also pointing out that "the regime simply loves to spin the sanctions as a tool of the 'evil' West, thereby inflaming the famous passions of a prideful Iranian populace and in the process totally avoiding all discussion of what actually led to those sanctions: the regime's own actions." Neal Ungerleider sees "stiff sanctions and fines" as the only viable solution to the issue, but he underlines that individual governments (the UK, Germany and Italy in particular), rather than the EU, can most effectively "put [the] pressure on firms to adhere to existing but loosely enforced laws." Paul Holman, Professor of Political Science and International Affairs at the University of Maine, also puts the onus on the parliaments of individual Western countries [rather than the European Parliament], urging respective legislators to "increase government spending on research and development aimed at deepening our knowledge of internet issues in Iran, China, Russia, Syria and other countries where cyber-activists are being suppressed."

If the ultimate goal is to standardise and refine the West's export policies with respect to Iran, would it be a positive contribution to that cause to leave the construction and enforcement of such legislation in the hands of individual governments with a range of economic strengths and political tendencies? The answer is no. It is inevitable that individual European Union Member States will have domestic priorities that affect international relations (Deutsche Welle 2012; Globe and Mail 2013). A national government is not necessarily all too different from a business conglomerate in that it has certain interests to protect. These interests do not always fully correspond to preserving and promoting human rights principles elsewhere. A

practical solution for this, as Kaeding and Voskamp (2011: 1) suggest, is "to turn to formal proceedings such as to the European Commission and its role as the guardian of treaties and treaty articles."

There have been many notable examples in the past (Rangelov 2013) when individual European Union Member States have taken inconsistent and contradictory positions regarding an overseas pro-democracy movement, resulting in a policy deadlock as well as the transmission of confusing signals to both oppressors and the oppressed. Such circumstances are hardly of much long-term strategic benefit to Europe or other democratic regions of the world.

Can the EU be more objective than the individual Member States? Perhaps not. But objectivity may be less important than consistently effective enforcement and sound ethics at this point. Feijt (2012: 10) insists that "neutrality and own interests are not combinable, since the interests of the EU are likely to influence . . . its neutrality in the mediation process." The inevitable truth is that in the case of any interference in a conflict by the EU, it "will be perceived as an enemy by the stronger party" (ibid: 10). Therefore, there may always be a temptation for Western powers to side with oppressive forces in favour of short-term peace and financial profit, at the expense of local justice. It should be noted as well that the dominant side of a conflict is not necessarily the numerically larger party. If the West sets democratic structure in its truly basic form as a primary measure of a movement's legitimacy and worthiness for assistance, the outcome can only be constructive for the grand scheme of international development. Once a commitment to assist has been achieved, the focus of policy can shift, as events develop, towards the protection of civil and minority rights through enabling religious and ethnic tolerance and bolstering an inclusive mode of political discourse based on free and open discussion.

Other surveyed experts, however, do not defend state-initiated economic sanctions. Dr. Soheila Vahdati argues that guiding policies should arise from the ICT industry itself, while Layla Hashemi raises the question of whether Western governments should have the right to intervene in the first place. Dr. Tessa Houghton questions any regional form of governance, arguing that the fault lies with the "global capitalist system which places profit before anything else." Adding that "there is a lot of discursive hypocrisy going on in this respect," she highlights the behaviour of Western governments that criticise censorship in repressive countries, but do not, for political or economic reasons, do anything tangible about tackling it.

Dr. Randy Kluver dismisses the European Parliament, not considering it to be an influential institution and viewing its capacity as strictly limited to symbolic moves. He argues that "if they try to impose strict controls on European or US involvement, then the Chinese will fill the hole." Dr. Jed Crandall, too, does not support any kind of government interference on the internet, but argues that Western governments should fund research into clarifying exactly what they can do, asserting that "if social media is to be an instrument of social change in places like Iran, we need a better notion of trust on the internet."

The significance of Dr. Crandall's acknowledgment of Social Sciences as offering valuable approaches to tackling the issue of censorship cannot be overemphasised. If constructively reinforced in the wider scholarly community, this perspective could have momentous policy implications for the European Union. So far, almost all technologically deterministic 'solutions' to internet repression that have been proposed in the West lack sufficient empirical and theoretical credibility. They rely on the assumption that telecommunications technologies

are inherently liberating. Meanwhile, occasional voices of reason, such as that of the techno-realist Evgeny Morozov of Stanford University, who frequently warns about what he calls 'the dark side of internet freedom,' have been drowned out by the overwhelming utopianism of most Western discourse on ICTs. Yet cynicism towards non-technical or multi-disciplinary strategies of change is not limited to Western computer engineers. Dr. Ulises Mejias remains highly sceptical of the viability of the use of legislation in regulating dual-use ICT exports, arguing that "the effectiveness of this approach remains to be seen, as the technologies that can be used for repression are the same ones that can be used for marketing."

There is some justification for many scholars' disbelief that the EU can have a positive impact on online political discourse in repressive countries. Nonetheless, its powers are far from negligible. According to op-ed written by Tony Blair and published in the Daily Mail (2013), "the EU is the most powerful political union and biggest business market in the world," meaning that if there is one single institution that can affect international politics, it would have to be the European Union. If we agree that the EU holds a considerable amount of political influence globally, then the only issue holding it back from achieving its goal of promoting democracy is its static, non-localised foreign policy. Even if the EU does take up this key policy role, obstacles will remain. The ICT industry is so dynamic that even EU Parliamentarians who are true digital enthusiasts will have a hard time keeping up with its pace of change. Add to that varying contextual dynamics in place in different repressive countries, and the result is an overly complicated situation requiring committees of expert consultants from an array of disciplines, ranging from computer networking to political and social and international relations, from law to cultural and religious studies. Yet any other more one-dimensional approach, especially one that is merely technical, is bound to fail, due to lack of insight into target countries' contextual realities as well as into doctrines and processes that underlie modern socio-political movements. Scrutinising the techno-political culture in Ukraine during the events leading up to the Orange Revolution, the next chapter aims to highlight the significance of cross-context empirical evidence to the critical analysis of large, complex socio-technical systems in undemocratic environments.

Telecommunications Technologies, Ethical Values and International Trade Policies: Towards a Comprehensive European Framework

A constructivist approach to STS encourages social realism by reinforcing the idea that socially motivated individuals and human networks have a fundamental leverage over technical trajectories, contingent on them operating under a democratic, accountable system (Burgett et al. 2013; Lins-Ribeiro 2013; Tavokin 2011). From a sociological standpoint, the perception that the ICT innovations' social impacts depend on what they have on offer, can only stem from a techno-utopian vision (Lewkowicz and Rohde 2011; Neff et al. 2012). However, when financial profit takes precedence to public welfare due to corporate choices, the European Union's altruistic values can be instrumental in protecting the human rights in vulnerable nations. Naturally, ethical values alone cannot automatically develop into incentives or enforceable obligations – at least not on a cross-border level. Therefore, the idea of a blanket policy mechanism seems increasingly vital to the establishment of a fair and dynamic international ICTs trade framework. This sensitive issue, which becomes consistently relevant every time the dual-use telecommunications technologies and intercontinental business agreements collide, has been called by Collins and Evans (2002) as "technological decision-making", and has various serious implications for democratic social organisations and movements worldwide (Sawyer and Rosenbaum 2000).

From a European perspective, there currently remains a regulatory void for a blanket framework ensuring a reasonable balance between generating profit and ensuring preservation of the core humanitarian principles and values on which the EU was founded (Golding 2000).

In a politically repressive context, the so-called technical decisions are not nearly as straightforward to implement as they are in the industrialised democracies. The inevitable alternative, in such countries, is not a nationally unified and functional system like those at work in open states, but instead a passive model in which major portions of the required innovations are eventually outsourced (Mansell 1999). Given this theoretical void caused by the predominantly Western themes running through the mainstream IS literature (Tenhunen 2008), the developing world's need for the promotion of technological ethicality seems (Som et al 2004) increasingly to be a significant one.

While the work of the classic Western scholars is known predominantly to form (Edwards et al. 2014) the foundation of STS as we know it today, some leading European politicians continue to justify their technological decisions based on a purely economic-driven framework known in engineering circles as "sound science" and "positive innovation" (ibid), which essentially aims to eliminate the notion of social corporate responsibility from the equation in favour of on-going revenue streams (Wartini and Heriyanto 2014).

Chapter v: Ukraine, China and the Arab Spring: Cyber-Activism and the Techno-Utopian Search for a Universally Transferable Model of Democratic Change

With an increasingly noteworthy ICT-mediated onslaught of information involved in modern social movements across the developing world, a comparative analysis of major case studies can indeed be helpful in illuminating certain grey points about Iran. The fifth chapter is dedicated to the scrutiny of ICTs' influence on modern pro-democracy movements occurred both before and after Iran's June 2009 presidential election, with a threefold focus on Ukraine's Orange Revolution, the post-reform China, and the Arab Spring phenomenon.

Ukraine's Orange Movement: Lessons in E-Revolution

The term Orange Movement refers to an array of mainly street-based, but predominantly peaceful, protests that took place in Ukraine, starting in November 2004 and ending in January 2005. The movement emerged shortly after the run-off phase of the 2004 Ukrainian presidential election, which was widely believed to be rigged by security officials in favour of Viktor Yanukovych, the sitting Prime Minister, at the expense of popular opposition candidate Viktor Yushchenko. The government first labelled the remarkably vibrant occupiers of Kiev streets as narcotics users bribed by the West, but a chain of persistent protests fuelled by the viral circulation of tasteful political satire drove the Ukrainian Supreme Court to intervene and invalidate the election results and order a revote. The repeat run-off in December 2004 resulted in Yushchenko's victory and was unanimously approved by independent observers as free from fraud. The movement faded later in January 2005, following Yushchenko's inauguration. The Orange revolution is known as the world's first successful political uprising to make extensive use of ICTs.

Although the true origins of cyber-activism during Ukraine's Orange Revolution are undocumented, it is widely considered among STS experts to be the world's first and most notable (Lysenko and Desouza 2010) example of a successful 'internet-mediated' political revolt. During the uprising various websites became central sources of information on breaking news locally as well as abroad, according to Hrycak and Rewakowicz (2009). As the Orange Movement flourished, Dyczok (2004) saw online news as the main source of information for professional journalists who relied on the internet to keep up with local events as well as global reactions to them. Kuzio (2005a) was possibly the first scholar of cyber-activism to call the Orange Revolution "the world's first" successful instance of its kind. According to Karatnycky (2005), this acclamation is well deserved in part because of constant online revelations of vast governmental corruption that came to be known as "the damning Kuchma tapes." A collection of other academic researchers, such as McFaul (2007), Noble (2008), Duffy (2010), Bozzoli and Brück (2011) and Zaluckyj (2012) have similarly endorsed the positive contributions of online media to this revolt, arguing that ICTs facilitated a wide range of political processes, including the announcement of voter fraud and the mobilisation, organisation and management of masses of discontented citizens. But much like the body of literature published on Iran's Green Movement and the Arab Spring, most scholarly assessments of the Orange Revolution remain technologically deterministic.

Nearly a decade on and many political revolutions later, we now know that the internet cannot be deemed an unbeatable liberating force. Web 2.0 has proven to be a non-bounded (Ashuri 2013), non-hierarchic (Chardy et al. 2012) means of communication, and is therefore

full of underexplored opportunities for any party prepared to take systematic, creative advantage of it. Yet the scholarly community must carefully steer clear from preconceived utopian biases common in some disciplines. For instance, Kuzio (2005b) attempts to connect Ukraine's popular uprising to the internet's ability to inject a "Western mind-set" into a younger generation through restless dissemination of "popular culture" and educational programmes. Harasymiw (2007: 12) simplifies the issue even further, claiming that the Orange Revolution "bore the hallmarks of its contemporary counterparts—a youthful, non-confrontational, and festive event making use of cell phone technology, the internet, and rock music . . . unlike the violent, bloody, and confrontational revolutions of an earlier generation in 1968." Although insightful in many ways, these two authors seem trapped in the excitement of 'post-revolution' journalistic literature. The fact that they are both of Ukrainian descent and the relative proximity of the dates when these studies were published to the height of the turmoil could have contributed to this theoretical void.

There are many similarities between the Orange Revolution and Iran's Green Movement in the patterns of how young political activists deployed telecommunications technologies. It will, therefore, be helpful to scrutinise the Ukrainian example, in search of a policy model for enhancing democracy in repressive states that might apply in multiple contexts. Lysenko and Desouza (2010) emphasise the importance of including the Orange Revolution in any STS study of post-internet social movements, referring to it as "one of the few globally important events" greatly influenced by telecommunications technologies. Examining the Ukrainian example is a generally overlooked necessity; they argue that by studying it, "we may learn relevant lessons and use them to build a general framework for the effective use of ICTs during electoral revolutions."

Despite a wide range of scholarly interest in the subject, the dynamic nature of the correlation between the internet and democracy remains insufficiently understood. Although the medium has been operational at the household level for nearly two decades, it was the emergence of Web 2.0 infrastructure that radically transformed its sociological influence. Yet Web 2.0 only spurred even more non-empirical, technologically deterministic literature. For instance, Filippova (2005: 138) suggests that this innovative and fully interactive generation of online technologies was, at least in the case of Ukraine, "a significant contribution to the development of [the] civil society and participatory democracy in ways not previously seen"—a largely techno-utopian assertion with no sociological justification of any kind.

Perhaps the most analytical study of the scope of the Orange Movement's engagement with ICTs is that conducted by Shyyan (2008: 96), who empirically examines Ukrainian dissidents' engagement with online technologies during the uprising. Having directly interviewed a number of prominent cyber-activists, he quotes one of them as saying that "the ability to operatively create and transmit information even under extreme conditions allowed us to save time and increase the effectiveness of our efforts greatly." Yet Shyyan does not fully clarify his sampling method. It is fair to argue that a cyber-activist previously subjected to state prosecution for their online activities might have elaborated on the medium's 'political drawbacks.' Shyyan found that techno-savvy Ukrainian cyber-activists tended to be predominantly "male . . . residents of urban areas [and] individuals with formal organisation memberships"—a pattern also detected by this research in the case of Iran's Green Movement. He blames the weak participation by female activists in online activism on factors such as "traditional organisational or leadership expectations of men rather than women in the Ukrainian society," and stresses "the need [for] civic awareness programs and youth organisations for the female population in Ukraine" as an effective solution. Yet he does not

put forward a detailed plan, or refer to Western policy as a potential option. Despite its originality and exceptionally rare non-deterministic approach to cyber-activism, Shyyan fails to establish a robust correlation between indicators of democracy like gender equality and the technological competence of the Ukrainian CIS, or even to acknowledge the existence of such a 'system.' This undermines the authority of Shyyan's conclusions.

Towards the end of the 21st century's first decade, a number of feminist scholars began addressing the routine lack of scholarly attention to democratic features of innovation systems at play in repressive states. For example, Hrycak and Rewakowicz (2009: 322) find blogging and internet publishing to be a central force in creating virtual feminist communities. Analysing such groups involved in the Orange Revolution and its aftermath, they assert that "at the core of virtual feminist networks are dozens of friends who are linked to each other through several communities concerned with feminism in Ukraine, most . . . based on the margins of academic institutions." Hrycak (2010: 165) argues that feminist tendencies and principles are now common not only among young female Ukrainian internet users, but also their male counterparts, and that "a new genre of creative writing called 'Zhinoche Pysmo' (women's writing) has vastly expanded discussions among intellectuals of the complex, contradictory situation of women in Ukraine." Complementary to Shyyan's fieldwork on the Ukrainian blogosphere, both of the above studies led by Alexandra Hrycak, Professor of Sociology at the Ukrainian Research Institute at Harvard University, could be the foundation of a thorough study of female cyber-activists' IT literacy, participation in innovation and the extent of their contribution to Ukraine's CIS.

Shyyan also investigates the extent of Ukrainian political dissidents reliance on ICTs—a prerequisite to determining their degree of innovation in this arena. He reports that "using the internet to advance one's political goals got agree or somewhat agree responses from 90.9 per cent of activists with significant international experiences and 70.3 per cent of activists who had not had such experiences." He also revealed that "none of the activists who had spent over three months abroad responded with a somewhat disagree answer to [the] item," and that deploying the internet for political purposes received "no less than 70 per cent of full or partial support" of the surveyed cyber-activists:

Ukrainian Dissidents and Internet Literacy

Survey Question	Yes	Mostly Yes	Mostly No	No	Total No. of Respondents
Do you know how to use the internet to support your political goals?	49% (37)	28% (21)	14% (11)	9% (7)	76

Table 17 (Shyyan 2008)

The disproportionate IT literacy rates among Ukrainian cyber-activists—in favour of expatriates—are a good indication of the extent to which 'political exiles' contributed to the Orange Movement's success. This may be due to the repressive nature of the ruling regime, which restricted local netizens' access to such technology. Inside the country, the Ukrainian government's censorship of traditional print and broadcast media during the unrest helped divert a mass audience to alternative, so-called new media, where accurate, up-to-date information was more readily available and where there were opportunities to participate in creating new information without facing as much risk of being silenced or censored (Way 2005). Reinforcing this observation, Ukrainian TV personality Ihor Kulias's (cited by Dyczok

2005) famously stated that obstructing the flow of information only works if the audience can be fully isolated, which is difficult and costly for repressive regimes in the post-internet era. "If the authorities monopolise a nation's media," argues Forster (2006: 14), "the opposition will likely receive no, or purely negative, coverage." Forster's position on the correlation between media censorship and innovative citizen behaviour is strongly supported by an array of cyber-activism scholars including Kyj (2006) and Duda (2010). This theoretical approach is more balanced, derives from an inter-disciplinary outlook and argues primarily that cyber-activists facing systematic censorship in repressive countries will either have to innovate their way through or look to foreign aid. Yet this perspective suffers from a critical conceptual gap: it fails to recognise that innovation processes are complex and deeply rooted in the socio-political contexts in which they occur. An innovation system comprised of highly motivated young professionals could still fail miserably, if it were to be deprived of basic requirements, including the free, dynamic flow of knowledge between its core structural elements.

At the time of the Orange Revolution, dynamic, fully interactive social networking tools as well as most advanced anti-censorship technologies were yet to be developed. The literature suggests that the Ukrainian government never systematically engaged in online censorship, perhaps because of the statistically low penetration rates of the medium across the Ukrainian population, who were mostly not computer-literate at that point. These factors may help justify the lack of evidence to indicate the existence of a single, vast, interlinked cyber-activist community in Ukraine at the time, let alone a separate innovation system involving cyber-activism such as the one at work in Iran today. The underdevelopment of user-oriented, Web 2.0 applications in the Ukraine coincided with the regime's inclination to dismiss the internet as an influential medium.

Regime censorship was countered through a number of static websites that helped Ukrainian protesters defy the national news monopoly, effectively neutralising the regime's attempt at an information blackout. Kuzio (2006: 56) argues that the internet functioned as an alternative to state-owned print and broadcast media, and that "the [Ukrainian] authorities never appreciated the power of the internet and had never been able to compete in [online] publications." McFaul identifies three main sites influencing the Orange Movement's success: *Ukrainska Pravda*, *Maidan* and *Telekritika*. According to him, "*Ukrainska Pravda* displayed the results of the exit poll most sympathetic to Yushchenko as well as detailed news about allegations of fraud. The website also provided logistical information to protestors . . . *Maidan* was a clearinghouse of information and coordination for protesters . . . [and] *Telekritika* emerged as a popular site for independent journalists during the campaign, and played an instrumental role in pressuring journalists working at Kuchma-friendly outlets to withdraw their support."

The 'anti-censorship' capacity of counter-publicity on the internet explains the Ukrainian dissidents' increasing reliance on ICTs over the months leading to the Orange Revolution. Venger (2006: 21) argues that, at the time, online media were particularly beneficial to local "journalists who were not afraid to be critical of the authorities and who were willing to give the public an alternative account of events." It is logical to assume that activist communities worldwide are most inclined to employ media where they expect to face the least censorship—precisely the case with the Orange Movement. Today, cyber-activism in Iran (and possibly elsewhere) has evolved from simply creating media that counter official narratives to include more expansive practices such as end users' active generation, employment and diffusion of technological innovations to counter systematic censorship.

This blurs the line between formerly disconnected concepts such as journalism, news consumption and advocacy in a much more thoroughgoing way than during the relatively early days of internet activism in Ukraine.

This convergence of roles, rather than a hidden trajectory within ICTs, is primarily why the traditional mass media's agenda-setting powers are increasingly irrelevant in the online sphere. The emergence of Web 2.0, in particular, has made interactions between oppressors and the oppressed much more dynamic. Today, the internet has given pro-democracy dissidents in repressive countries a voice—and consequently made them more vulnerable to prosecution. When scrutinising the relationship between ICTs and activism, the main intellectual emphasis, therefore, should always be put on the system in which a given community engages with online innovations, rather than on conveniently assigning a particular political rhetoric to telecommunications technologies, which are the product of complex socio-technical processes and often neutral by nature.

According to Polyuha (2005), internet use grew by forty per cent during the months of the Orange Revolution. Mussuri (2005) also confirms a significant boost towards ICT-mediated forms of communication in Ukraine via an analysis of the donor support system available to the country's mainstream media. Tying it to Habermas's theory of public sphere, he suggests that "the public sphere has ideal conditions for discussion if every subject with the competence to speak and act is allowed to take part in a discourse, allowed to question any assertion, allowed to introduce any assertion and allowed to express his or her attitudes, desires and needs, and if no one may be banned from talking or coerced from talking." Venger (2006: 22) holds that ICTs can serve dissent and repression equally, depending on how they are employed, asserting that "the media represent resources that can be mobilised to demote or promote democracy." What he describes as the "triumph of the [Ukrainian] opposition on the internet" was largely due to its active employment of spontaneous, bottom-up and context-driven techniques emerging from the core of the Orange Movement—a valuable advantage compared with the regime's failure to adequately re-strategise and adapt to the internet in a timely, efficient manner. This, according to Lysenko and Desouza (2010), led to the formation of an "Internet-based public sphere in Ukraine," where professional and citizen journalists suddenly found themselves free from censorship.

Today, it is evident that the Ukrainian government, unlike most authoritarian regimes today, did not take the internet seriously enough to systemise its regulation, and gave precedence to more traditional forms of 'news media.' This model of cyber-conflict cannot be applied to Iran, where the regime has a strong, systematic online presence. This indicates that when it comes to the internet, repressive regimes can learn just as much from history as democratic movements. The Orange Movement's pioneering use of ICT-mediated means of protest was no less of a valuable example to Iran's Green Movement than was the Ukrainian regime's inability to acknowledge and utilise such technologies in an effective and timely manner an example for other regimes of what not to do in similar conflicts. Kyj (2006) likens the scope of the pro-Yanukovich camp's online activity to that of a "student group" using the internet casually and to address its daily chores. Only half a decade later, the internet was at the centre of Iranian security officials' war on dissent.

The Ukrainian regime overlooked the 'security threats' of online media—and indeed only between three to eight per cent (Mussuri 2005) of the Ukrainian population was estimated to have regular access to the internet at the time. Given the government's firm control of the country's print and broadcast media, the situation appeared deceptively in hand. But the

immediate reach of a medium is not necessarily always the most useful indicator in determining its penetration rates within a given community. According to Kyj (2006: 79), in Ukraine the internet's "ability to simply get [the] information out to a limited audience was enough to set, in motion, a ripple effect." Lysenko and Desouza (2010) theorised this via extensive empirical scrutiny of cyber-activism in the Orange Revolution, arguing that online media's influence on the Ukrainian public, despite poor connectivity rates, was relatively high. This, they argue, happened in part because the first generation of the country's netizens were university "students and professors, young employees of the international and big national enterprises, collaborators of the research institutions, journalists [, and] politicians"—those perceived to collectively carry the most weight in determining the trajectory of social movements.

On a political level, although there are a number of fundamental similarities between the Orange and Green movements, it is important not to ignore the differences between the systems they opposed. For instance, there are clear structural distinctions in the repressiveness of the two regimes. The Ukrainian government was, as Dyczok (2006: 224) describes, a "semi-authoritarian [system, which] allowed certain media outlets to exist," whereas its Iranian counterpart is an ideology-driven military dictatorship. The scope and dynamics of interaction between local and expatriate cyber-activists and the age composition of activists are other noteworthy areas where the two movements differ greatly. Explaining that a dominant portion of active political protesters in some autocratic states such as Iran tend to be in their late twenties and early thirties, Lysenko and Desouza (2010) argue that the internet "can have even higher [democratising] potentials" when users are predominantly young. Yet these scholars see the incapability of the Green Movement to "rouse the wider international circles to action," as the main reason behind its collapse, linking it to external factors including the "relative weakness of the Iranian diaspora worldwide"—an issue with much less impact in the case of Ukraine.

This breakdown, however, cannot be solely laid at the feet of the interactional structures and patterns within the Iranian cyber-activist community, as Iran's 2009 turmoil is known to be the first time in history when a ruling elite went as far as 'pulling the plug' of the internet. The regime complemented the internet blackout by shutting down cell phone networks, blocking all outgoing international calls on landlines, and boosting its jamming of the satellite TV signals. Here is a crucial fact often ignored by some overenthusiastic advocates of online revolution—when the internet goes down, theories of cyber-activism, most of which are based on technologically deterministic premises, will cease to be applicable. This is precisely why an Innovation Systems (IS) approach is realistically relevant and needed in repressive contexts. Even if external actors were to offer a stable, tamper-proof, and high-speed parallel network connection to a given cyber-activist community in a repressive country, it would still be quite difficult and hazardous to verify the identity of the clients taking up such a service. A fully open network might coincide with the strengthening the regime's bandwidth and furthering the capacity for online crime—the main reason why most techno-utopian solutions for repression have failed to date. Such a 'solution' would compare to providing anti-regime forces in repressive countries with deadly weapons without a chance to verify the legitimacy of the recipients, who may well turn out to be vicious villains. Just as Western countries have been vexed by moral questions regarding arming rebellions against murderous dictators, technological interventions in online power struggles do not necessarily have straightforward impacts and consequences.

Despite various demographic and educational advantages over Ukraine's pro-democracy dissidents, Iranian cyber-activists are less likely to achieve their aims, as they face a much more ferocious challenge: to overcome a secretive police state with plenty of resources to invest in foreign technologies. It is, therefore, vital to the democratisation process that Iranian cyber-activists' counter-innovations continue, as continued filtering and blocking of information will weaken dissent. Idealistic obsession with any particular online platform can only distort the process by ignoring societal factors that enable technological innovations. Lysenko and Desouza (2010) noted an overemphasis in the academic literature on the role of Twitter in Iran's Green Movement, reminding some commentators that security officials would have been foolish not to have individually processed all those public Tweets, many of which contained valuable details about the time, location, and scale of street demonstrations as well as the identities of organisers and participants. They suggest that "the Iranian opposition might have been better served by utilising more secretive technologies, as excessive information openness can sometimes play a negative role in events which naturally require some secrecy."

Green Movement activists were also less able to attract external attention than their Orange counterpart, and Ukrainian cyber-activists benefited considerably more from foreign (i.e. Western) assistance. Often provided by Western NGOs and governments, humanitarian aid has historically varied from financial to technological to educational assistance. Some of the institutions making contributions to the Orange Movement include, according to Karatnycky (2005), the United States government, the European Union, "the National Endowment for Democracy and private philanthropists such as George Soros . . . [reinforcing] democratic values and [deepening] the public's understanding of free and fair electoral procedures." Many scholars including Kyj (2006), Polese (2008) and Duffy (2010) argue that the Orange Movement managed to successfully engage with advocates of democracy in the West through the internet, convincing them to help promote the cause either by travelling to the country to join the protests, or via making online financial donations to designated e-commerce accounts. Zaluckyj (2012: 25) relates that he sees the internet's 'democratic powers' in its capacity to offer a real-time "view from the trenches," stirring emotions and provoking excitement among foreign sympathisers of a revolt, who are able to "see and share the experience simultaneously." But she seems to give too much credit to this emotionally-driven viral effect. A similar phenomenon occurred during the Arab Spring—a wave of pro-democracy movements characterised by severe internet censorship.

Arab Spring: Dawn of a Revolutionary Model or Dusk of a Techno-Utopian Dream?

The extent to which ICTs were instrumental in the Arab Spring protests has not been examined in sufficient depth. Arab political activists reportedly resorted en masse to solutions allowing "secure online communication" (Hintz 2012: 95) during the revolts in question. Apart from journalists and scholars (e.g. Bresheeth 2012) who were fast to refer to the protests as 'unpredictable,' the relatively limited range of empirical investigations on the issue have largely explored conventional territory, failing to build constructively upon conclusions from previous case-studies, or to delve into underlying contextual factors influencing online mobilisation in emerging economies. What Ergul (2012: 1) refers to as the transformation of a common man into a "cyber-society effective in world politics" via new telecommunications technologies, may have deep roots in non-technological undercurrents, and may well be more efficiently explained from a constructivist perspective. If the relatively short history of cyber-activism has taught us anything, it is that there is very little need for pre-conceived, deterministic biases in the field of STS.

The main framework that social scientists consistently employ in most assessments of contemporary Arab movements is Social Movement Theory and its surrounding concepts. Some have proceeded to combine the theory with much more contemporary theories of cyber-activism and online communities in smart, creative ways. Yet insisting upon an entirely sociological approach with only limited understanding of online technologies would be just as damaging and fruitless as pressing for techno-utopian methodologies.

While many of the models developed by researchers for the concept of politically motivated cyber-activism are theoretically useful and well justified, they incline to label movements in terms of specific technologies involved and are quite bounded by national contexts. By undertaking a dynamic, Innovation Systems approach, it should be possible to not only gain a more realistic perspective on the interplay between social movements and ICTs, but also to draft a broader model which could be extended to a wider range of political contexts. In order to achieve such a framework, scholars working in the field must closely examine, fully comprehend and analytically compare contextual characteristics of repressive states worldwide. There is a demand for STS research to shift from focusing mainly on just technology or only social processes to new approaches in order to develop a systematic explanation for how the two interact in repressive environments.

Among the most notable aspects of the Arab Spring protests were the varying degree of repression that different regimes deployed against protesters and the inconsistent measures they were prepared to take in tackling their opponents. Yet the failure to address this in much of the literature, along with other significant conceptual gaps on matters such as the history of political activism, the penetration of higher education, the demographics of the population, and cultural attitudes towards new technologies and rights of women and minorities, justify Chokoshvili's (2011) criticism in calling the often heated debate over the absolute effectiveness or outright redundancy of the ICTs to political revolutions "a superficial one."

The technological infrastructure of a country and the technological literacy of its population are influential in affecting the extent that ICTs can help a social movement in a repressive country. Currently, the average connectivity rate in the Middle East ranges quite widely—from a mere five per cent in Iraq all the way to ninety per cent in Qatar. Interestingly, most scalable Arab Spring protests took place in countries with relatively high connectivity rates and predominantly young, educated populations. Yet it is crucial to always put the use of

ICTs in context. Otherwise, we would, as Wilken (2012: 188) argues, be ignoring "the longer history of technology use in political protest, as well as earlier forms of political protest and pre-digital social networking." This approach is supported by Ekwo (2012: 3), who draws the scholarly community's attention to the fact that "we have lots of instances of dictators overthrown before Facebook." The fact that the Arab Spring protests took place in countries where poverty, unemployment, inflation and inequality had reached record highs coupled with declines in GDP growth (Dewey et al. 2012), makes it evident that dissent has, as Stepanova (2011: 1) argues, a lot to do with "underlying socio-political and socioeconomic factors behind" what is sometimes mistaken for a 'purely online' phenomenon.

The assumption that people with regular internet connections have more political powers than those without misleads scholars. Such an approach not only leaves itself open to the question of whether the same proportion of the population would still have been as politically active in a hypothetical absence of online technologies, but also ignores empirical evidence suggesting that cyber-activism has, in many instances, facilitated the identification and arrest of dissidents by repressive regimes. Such thinking also discounts the role of 'offline' protesters, such as Iran's Labour Movement and the Mothers of Laleh Park, who have been instrumental in forming and developing the country's pro-democracy movement(s). In such a technologically deterministic model, Mejias (2012: 147) suggests that for any noteworthy change to occur "everyone must be connected to the same digital networks." Perpetually putting the emphasis on digital networks as opposed to people "can . . . serve to obstruct any real critique of social media technologies, and to justify their use without the need to question their terms of use."

Apart from superficial approaches and common exaggerations regarding the role of ICTs in Arab Spring protests, inept methodological designs and analytical frameworks mar some studies. Relative limitations of the literature include relying on unverifiable sources, making unsubstantiated claims, asking irrelevant interview questions, lacking contextual familiarity, exhibiting pre-existing bias and failing to triangulate data. Aday (2012: 15) likens the common emphasis on easily accessible data (as opposed to data best suited to the research) to "the proverbial drunk searching for his lost key under the streetlight because that is where he can see." The blatant forfeiture of accuracy in favour of convenience can subsequently lead to the exaggeration of the "size of the audiences . . . [failure] to grapple with the many differences [existing within] . . . the broader population of citizens" (ibid), as well as overestimation of the political significance of online social networking platforms such as Facebook and Twitter.

An empirical comparison of the innovative use of ICTs by Arab Spring protesters with that of their earlier counterparts in other parts of the world (especially central and eastern Europe) has so far been an extreme rarity in academic literature. This is perhaps due to the scholarly world's preoccupation with surface-level cultural similarities. The overemphasis on the contextual resemblance between the Arab states and Iran by some researchers has not, so far, resulted in any significant theoretical advances. It is sensible to assume that every political opposition movement seeks to learn from its predecessors regardless of geographical boundaries—as might repressive regimes as well. But Chokoshvili's (2011: 32) assertion that "Arab states with access to ICTs had been influenced by the success of Western democracies long before the 2011 revolutions," is, on its own, inspiration enough for a comparative analysis of two of history's most analogous post-internet mobilisation waves, namely Iran's Green and Ukraine's Orange movements.

While ICTs have historically proven to be useful to revolutionary movements, they have also shown themselves to be just as helpful to repressive states in combating dissent. Given the vast range of valuable resources many repressive regimes tend to control, they often have no financial reservations about resorting to costly foreign expertise in order to implement censorship plans. Evidence has revealed that an array of dictatorial regimes including Iran, Burma, China and Egypt have been routinely assisted in online censorship by Western telecommunications companies such as Cisco, Motorola, Boeing, Alcatel-Lucent, McAfee, Netsweeper, and Websense (Mejias 2012). The pattern detected in dictatorial regimes' reliance on Western technology draws attention to existing international regulations on technology trade, raising serious concern over academia's increasingly excessive focus on technology itself, as opposed to policies aimed at "changing the legal environment," as articulated by Hintz (2012: 96).

Although Western firms' coordinated abstinence from cooperating with repressive regimes would be generally helpful to the democratisation process in the respective countries, ensuring consistent, timely external pressure at the time of political unrests can be another valuable lifeline to a pro-democracy movement, provided that such pressure meets other basic criteria determined by social and political scientists. This form of intervention, as Chokoshvili (2011: 23) acknowledges, makes "violent crackdowns or extreme human right violations . . . less likely." More importantly, the impact of such technological intervention seems to be more considerable in fully authoritarian states than in those where repression takes a milder form.

Absolute dictatorships thrive on the blockage of information—breaking such blackouts can cause rapid destabilisation of ruling elites. These regimes, as Dewey et al. (2012: 4) observe, lack "appropriate feedback mechanisms that could warn them of the depth and characteristics of popular discontent, [and] are frequently incapable of identifying and addressing social unrest in a timely manner." Semi-authoritarian regimes, by contrast, tend to be more prepared for systematically combating dissent, perhaps because they face more educationally competent and persistent opposition. Semi-authoritarian regimes vary enormously, however, and include ones based in ideology like Iran, populist governments like Venezuela and even rich, sparsely populated Arab states like the UAE, where the regime's strategy relies on politically de-motivating the citizens by keeping them economically contented (Stepanova 2011).

While many scholars have argued for and against the idea that Iran's Green Movement was a political precursor to the Arab Spring, there is no proof to suggest that the protesters in the latter movements used or built upon technology developed by or for Iranian cyber-activists in the period since 2009. More importantly, there seems to be no record of any anti-censorship software specifically designed for the Arab context. This could be due to a number of factors, such as some Arab governments refraining harsh forms of online censorship (like in Iran and China) in the face of international pressure, and/or an underdeveloped cyber-activist community in those countries. As a result, the primary focus of researchers working in this area will need to be redirected from a 'predictive' mode to one of analysis, relying on concrete empirical evidence and contextually informed, academically proven concepts and models. Otherwise, as Ergul (2012: 1) warns, discourse will never go "beyond an essentialist approach subsumed under the primacy of inconsistency between Islam and democracy,"—a misleading, unconstructive supposition at best.

With a careful, methodical comparison of modern political movements in the undemocratic world, as well as close examination of the social contexts from which they tend to arise, it would be possible to develop a more inclusive policy framework in favour of the global promotion of democracy, or at least, as Stepanova (2011: 4) suggests, to transform online technologies into "a qualitative accelerator in the context of present or future protests" in repressive states like Iran. Unless such changes proceed, we will not be able to learn from the past, and our understanding of the interplay between technology and politics in repressive countries will, in Aday's (2012: 16) words, continue to suffer "from the same flaws as accounts of Iran's Twitter revolution, leading to faulty policy responses and unwarranted expectations." This also lies at the heart of why the West's reaction to the Arab Spring protests was not, in any significant way, timelier, better organised or more helpful than its response to Iran's Green Movement.

Hi-Tech Telecommunications, Political Openness and Security Initiatives: The Case of Post-Reform China

Today, the Chinese economy is regarded by some in the West (e.g. Dahlberg 2014; Wade 2011) as highly developed, and an imminent threat to the global commerce leaders. However, the question remains if a top-down, pre-planned innovation system, however lucrative, can be truly deemed as a sustainable, socially just model for economic governance. The core issue with the revenue-driven rationale has been occasionally highlighted by the policy reformists worldwide (e.g. Van Berkel et al. 2012), which makes the Chinese model seem even further questionable in nature. If a successful economy were to be defined merely by its levels of financial income, then how can we distinguish an act of virtue from a morally illegitimate endeavour? Democracy can be portrayed in many different, and sometimes contradictory, variants. For instance, Habermas (1996; 2003) perceives democracy to be the provisional outcome of an on-going, negotiated political process. Nevertheless, the core principles of the Habermasian political ideology do not seem to hold as firmly when translated into the new generation of the telecommunications technologies. The rationale of Habermas misses a key STS principle: that even the most 'democratic' ICTs, as we know them, can often equally facilitate repressive ends. If there is one sociological lesson to be taken away from the online era, it will be that democracy can be a surprisingly fluid and unstable notion when applied to the virtual world (Laskowska 2014). While some of the internet's liberating promises continue to make sense in a broad range of terms, one cannot afford to overlook the socially decentralising effects caused by it as an interactive, participatory mass medium.

Having essentially followed the Soviet Union's footsteps especially on the issues surrounding hard sciences and defence industries, China's communist party has an extensive history of approaching the technological innovations from a highly centralised, top-down position. However, since the major reforms undertaken during the 1980's, the Chinese regime has opened up the country's manufacturing sites to the West, causing a radical shift (Leydesdorff and Guoping 2001; Liu and Lundin 2007; Xiwei and Xiangdong 2007) in its previously constrained economy.

Despite some right-wing Chinese critics labelling the communist party's liberal market changes as an irresponsible open-door policy, the reforms in question inspired the country's universities to actively seek more links with the local and regional industry leaders, as well as with leading Western research centres. However, according to Sun and Liu (2010) China's NIS continues to face two main disadvantages when compared to its Western competitors: the still very tangible control of governmental agencies over the otherwise independent

academic research projects, and the extensive role of non-sovereign, politically subsidised institutions in the nationwide R&D planning. During an enlightening study, Motohashi and Yun (2007: 1251) propose that, even in the post-reform China, the public and private sectors were "completely separated" in terms of R&D planning and research objectives.

Perhaps a conveniently overlooked fact when it comes to the post-reform China is the government's reservation of the right to have mandatory representation on the directing board of nearly every large company across the nation. Under such dynamics, which is what Guan et al. (2009: 802) refer to as "preferential treatment", big profitable businesses are left with no choice but to pretend to "be conservative and value security over innovation" (ibid: 802) at all times.

These top-down business practices are an everyday issue in the post-reform China. For example, Lu (2001: 930) argues that although the NIS theory has been designed to help ensure the functionality and advancement of national economies, the non-organic way in which states such as China have approached innovation has led to a self-restrictive system in which the "uppermost strategic resources [are] used, adjusted and controlled by the state."

Another critical characteristic of the emerging economies overlooked by mainstream NIS is the often highly politicised nature of the domestic R&D firms and regulatory mechanisms. The mere quantity of the R&D budget in a given state cannot necessarily be a valid indication of its sustainability or self-efficacy. China and India, for instance, have been turning increasingly into "important sources of information technologies [by attracting] many multinational companies to set up R&D laboratories" (Sun 2002: 1060) within their borders, and subsequently by allowing them to "dominate [their] high-tech exports" capacities in strict accordance with their own industrial requirements (Sigurdson 2004: 5). The third world regimes' excessive focus on foreign expertise tends to have an adverse impact on their privately run local enterprises. In the case of China, for instance, there is a "significant productivity depression" (Fu & Gong 2008: 8) following the communist party's economic reforms in the 1980s. Moreover, the sheer volume of a nation's innovation system's output on its own cannot be a determinant of its full functionality, and "openness to competition and the intensity of spending on higher education are particularly important" to the genuine, bottom-up economic progress (Wu 2007: 548) – a crucial essence fundamentally missing from the NIS in repressive countries like China and Iran.

In South East Asia, tight production deadlines have become much more relevant to the mass economy than endogeneity of the academic output. The excessive focus on adaptation rather than innovation of advanced scientific knowledge, according to Sun and Du (2010: 542) is a direct consequence of the Chinese NIS being historically "plagued with many problems due to the legacies from the [communist regime's] planned economy." To unveil the real state of the ICT industry in the post-reform China, it suffices to mention that the communist party's online censorship apparatus "relied on 100 per cent of its acquisition of telecommunication equipment through imports" (Fan 2006: 361), while the genuinely private enterprises have been wiped out or ignored (Kanamori et al. 2007: 2) in "official thinking about technological issues." From the Chinese regime's standpoint, big business objectives must be "better met by the less risky course of procuring advanced technology from abroad" (Suttmeier et al. 2006: 59).

The NIS theory in its classic form also does not determine (Gu and Steinmueller 1997) the healthy extent to which the political administration can or should interfere with a country's knowledge generation processes in relation with the Triple Helix model.

The definitive solution to the conceptual shortcomings of NIS in relation to repressive states does not seem to lie in seeking a blanket framework aimed at addressing the world's censorship issues all at once. On the contrary, the main emphasis needs to be removed from theorising the so-called 'transferrable' social influences of ICTs, and instead to be placed on the "comparison of alternative system-level structures and their relative strengths and weaknesses . . . , [as well as the] differences in initial starting conditions" (Liu and White 2001: 1092). Otherwise, the Chinese model will continue to be the emerging economies' best future hope.

This is not to insinuate that the Chinese universities are not investing sufficiently in academia, but that the universities in China are held back by the same inward, technologically passive culture largely incompatible with the key actors originally outlined by the NIS model. Therefore, the country is largely bound to remain a "political economy characterised by active governmental involvement in business, both through ownership and through regulation" (Deng 2007: 72) or, as Gu et al. (2008: 11) put it, through "extraordinary rates of savings and capital accumulation," instead of by endogenous knowledge production.

As a consequence of this reactionary approach to innovation, the political regimes in the emerging economies often choose to exploit imported technologies over indigenous expertise. This is chiefly due to their strong inclination to satisfy the global market, and to fulfil their finance-driven schedules. As Tan (2010: 2917) argues, it is exactly this "lack of innovation process that makes emerging and developing countries stay undeveloped."

The fundamental difference between the processes involved in functional innovation systems where the concentration is on originality, and the so-called catch-up economies whose ultimate goal is to understand, employ and at the very best improve on imported technologies, marks a clear doctrinal division between the two models, suggesting strongly that the inductive patterns often "emerging from geographic studies of Silicon Valley or the City of London are inadequate for development of general theories" (Miao et al. 2007: 714) when it comes to the democratic implications of ICTs.

This research argues that the recent pro-democracy movements in Ukraine, Iran, the Arab states and even China could have been more rigorously supported by Western, democratic governments, had they recognised the potential of supporting the CIS in such nations. The next chapter will examine some of the policy solutions that may help promote democracy in repressive countries.

Chapter vi: Fostering Democracy—Western Export Control Regimes, Corporate Social Responsibility and the Technology of Repression

The widely documented contribution of Western ICT companies to online censorship in repressive states highlights a need for a Europe-led, more robust global regulatory system to control the exportation of dual-use technologies. The sixth chapter focuses mainly on assessing the policy implications of the results of this research, drawing on specific recent examples as gathered via weblog content analysis and document reviews.

The ethically dubious business conduct of European ICT firms in conflict zones has come to the attention of high-ranking European Union politicians, some of whom found NSN's business activities in Iran inconsistent with policies to promote human rights and democracy in repressive countries. According to Cheng et al. (2011), in a meeting that took place on 8 July 2010 in Paris, French foreign minister Bernard Kouchner and Dutch foreign minister Maxime Verhagen "recognised the complicity of European corporations in the Iranian crackdowns, and proposed an international agreement on restrictions to impose on private companies with regards to high-tech censoring equipment." The French company Alcatel was also accused in the same meeting of having sold similar technology to the Burmese regime. Similarly, "[United States] Senator Dick Durbin . . . proposed a bill penalising this conduct by American corporations" (ibid), which was more enthusiastically received. The problem is not a lack of regulation, but the complete void of a systematic legal mechanism to consistently enforce ethical business conduct across Europe.

Trade Regulation, Western Policies and Power Struggles in Repressive States

A European Commission (EC) regulation from 5 May 2009 acknowledges an immediate need to control dual-use technology exports. It clarifies that "dual-use items shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices." It further explains that restrictions on 'dual-use ICT' refers to the "transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone." While the EC has tightened its definition of dual-use technology when compared to a previous act adopted on 22 June 2000, in practice, the focus is predominantly on the exportation of innovations potentially useful in conventional military projects, such as the production of weapons of mass destruction. The need to develop a mechanism that acknowledges 'soft power' efforts as dangerous threats to humankind remains largely to be addressed across the region. In its latest move, the EC introduced a green paper on 30 June 2011, in which it suggests a number of significant improvements on the mechanism of control over the exportation of dual-use technology by its member states. Yet the exportation of dual-use ICTs to many repressive states in the underdeveloped world remains a serious problem. Current policy gaps have resulted in companies such as NSN finding legal justifications for engaging in behaviour that current regulations mostly frown upon, rather than forbid.

Interestingly enough, even from a purely financial perspective, engaging in business contracts with repressive regimes has not been a viable long-term strategy for Western companies in many instances. Sohrabi-Haghighat and Mansouri (2010: 32) observe that the revelation of NSN's alleged contribution to online censorship in Iran "resulted in considerable reduction of [the brand's] sales in Iran." While it is estimated that NSN's co-operation with the Iranian regime has cost the company somewhere between a quarter to half of its business in the country on a permanent basis, there is no evidence of their products and services having been boycotted in any other part of the world in solidarity with the Green Movement of Iran. Dawoody (2011: 16) also suggests that unethical technology sales ultimately harm the firms involved, arguing that "these types of businesses suffer from poor public relations through boycotts which force stakeholders rethink such endeavours in the future." The emphasis on the importance of an ICT firm's stakeholders is particularly noteworthy given the global search for a practical approach to dubious technology trade. Sturges (2010) spots a "capacity for the corporations to be questioned [by their shareholders] on the ethical dimensions of their policy which could be taken up by freedom of expression campaigners." Informing shareholders can be an effective way of influencing an ICT conglomerate's policies at minimum financial and political cost.

Pressure from international human rights NGOs on European Union officials over the international business deals of NSN, Alcatel and Ericsson and other European companies persuaded the European Parliament to pass a resolution on 10 February 2010, stating in part:

[The] European Parliament strongly criticises international companies, in particular Nokia-Siemens, for providing the Iranian authorities with the necessary censorship and surveillance technology, thus being instrumental in the persecution and arrest of Iranian dissidents.

Russian news agency Ria Novosti cited a UN press release in 2010 announcing an EU decision to call "on the Iranian authorities to stop the jamming of satellite broadcasting and Internet censorship and to put an end to this electronic interference immediately." Xindex (2013), however, urged the EU to make a more concrete move to promote digital freedom abroad, arguing that "self-regulation and corporate social responsibility often do not go far enough to adequately address this issue." In an online article titled "Outwitting Iran's Cyber Censors," European Voice (2010) asserts that the EU and its member states should employ mandatory rather than voluntary measures, requiring companies to preserve human rights in dubious states, affirming that "the EU also needs to help Iranian civil society to unblock existing channels of communication or create new ones." Yet the EU needs to consider the contextual realities of individual nations before further developing its international anti-censorship policy, so that it does not merely attempt to extend laws generally accepted in the West. To give an example of potential complication, according to the Financial Times (2008), one way Iranian youth defy governmental censorship is through sourcing bootleg DVDs. While such products are considered outright illegal violations of copyright law in Western states, they are viewed as 'cultural gems' in countries subject to censorship and repression, where the only way to catch up with the international arts scene is through 'illegally retrieving' what would otherwise remain out of bounds.

Western lawmakers need to consider the cross-border effects of not only their foreign policy, but also their internal policies when it comes to ICTs. One prominent recent example was the attempt to pass the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) in the

United States Congress—a law, which despite all its alleged 'legal' benefits, would have offered a crushing blow to cyber-activists operating in Iran and in other repressive states.

The following table briefly compares some of the potential effects of the SOPA/PIPA and other similar proposed legislation on civilian lives in the West and in many underdeveloped, repressive regimes:

Implications of 'Anti-Piracy' Policies: Western Democracies vs. Repressive States

Typical Western Users	Cyber-Activists Residing in Autocracies
Some websites would be blocked	TOR would be blocked
Email providers could be forced to censor certain links	Alternate DNS would be disabled
Content shared on SNSs would be monitored and censored	Proxy servers located in the United States and used in countries like Iran would become inaccessible

Table 18 (Atlantic Wire 2011)

Case Study: Nokia-Siemens Networks and the Iranian Market

It was revealed in the aftermath of the 2009 Iranian presidential election that the Finnish-German ICT firm Nokia-Siemens Networks (NSN) had sold a number of potentially repressive products and services to the Telecommunications Company of Iran (TCI), including mobile voice recognition technology that the government repeatedly used to track down and arrest political opponents. It further helped the regime set up a comprehensive internet censorship system. Between 2009 and 2010, angry consumers worldwide, who were sympathetic towards the protesters, as well as many European politicians, began to put pressure on the company. Costly consumer boycotts along with open criticism of the company's activities in Iran from the European Parliament, as well as a lawsuit filed in the United States District Court for the Eastern District of Virginia against NSN by the legal representative of an imprisoned opposition figure, persuaded company officials to shift from denying the issue to acknowledging a major error on their part. In a public statement, the company subsequently promised to thoroughly revise its business codes for conduct in undemocratic states such as Iran, where it admitted NSN technology had been systematically employed by the regime's security officials to silence legitimate dissent.

NSN and Policy Lessons for the Future: An Analysis

On multiple occasions, NSN has officially responded on its international website to worldwide accusations of allegedly unethical business conduct in Iran. These responses can be divided into three main categories of denial, legal justification and finally admission and apology, which may indicate the relative power of public shareholders in Western political and economic structures. The following statement hails from NSN's (2009) first written response to the issue as found on its online database:

Nokia Siemens Networks has provided lawful interception capability solely for the monitoring of local voice calls in Iran. Nokia Siemens Networks has not provided any deep packet inspection, web censorship or internet filtering capability to Iran . . . The restricted functionality monitoring centre provided by Nokia Siemens Networks in Iran cannot provide data monitoring, internet monitoring, deep packet inspection, international call monitoring or speech recognition. Therefore, contrary to speculation in the media, the technology supplied by Nokia Siemens Networks cannot be used for the monitoring or censorship of internet traffic.

Pressure from the European Parliament, international media and human rights advocates, including the Iranian Nobel Peace Prize winner Dr. Shirin Ebadi, mounted after a lawsuit was filed against the company in the United States District Court for the Eastern District of Virginia by reformist political figure Isa Saharkhiz, who claims he was located and arrested after briefly turning on his old regular cell phone while in hiding. The lawsuit was quickly followed by an inquiry launched by NSN shareholders, which led company officials to acknowledge the error. Yet as evidenced by the following statement, NSN continued to justify its contracts with Middle Eastern dictatorships:

It is true that all modern mobile communications networks include a lawful interception capability; this capability became a standard feature at the insistence of the United States and European nations. These countries needed the capability for law enforcement reasons that are common throughout the world. It is unrealistic to demand that wireless communications systems based on global technology standards be sold without that capability. (NSN 2010a)

The company eventually revised its business approach in Iran, took full responsibility for enabling the IRGC's abuse of its communications technologies and services, condemned online censorship in Iran and agreed to pull out of Iran at the next opportunity. At least four separate, official apologetic statements were published by NSN on its website during 2010. Here are some crucial extracts:

Nokia Siemens Networks is aware of credible reports that the Iranian authorities use communications technology to suppress political activity in a way that is inconsistent with that government's human rights obligations. As a result of these credible reports, Nokia Siemens Networks halted all work related to monitoring centres in Iran in 2009. Nokia Siemens Networks divested its monitoring centre business in 2009 and will no longer provide monitoring centres to any country. The company has voluntarily restricted its business in Iran by not seeking or accepting new customers and by limiting its activities with its current customers. Prior to providing a monitoring centre to an Iranian mobile operator in 2008, the company believes it should have better understood the possible implications for human rights in Iran. (NSN 2010b)

We share a concern for the welfare of dissidents and journalists persecuted for free expression in Iran and elsewhere. Accordingly, we call upon all countries to follow due process and provide humane treatment in accordance with their laws and applicable international agreements. (NSN 2010c)

Nokia Siemens Networks provided to Iran one monitoring centre necessary for effective use of the legally mandated lawful intercept capability . . . Nokia Siemens Networks's monitoring centre business was a small unit that, at the time of its transaction with Iran, was slated by Nokia Siemens Networks for sale because it was determined not to be an essential part of our core business. Nokia Siemens Networks divested its monitoring centre business in 2009 and no longer provides monitoring centres to any country . . . We do believe that, ultimately, the governments that misuse communications technology must be held accountable for that misuse. (NSN 2010d)

While we do not intend to enter this business again . . . we halted all work related to monitoring centres in Iran in 2009, including service and support, we believe that we should have understood the issues in Iran better in advance and addressed them more proactively. There have been credible reports from Iran that telecommunications monitoring has been used as a tool to suppress dissent and freedom of speech. We deplore such use of a technology . . . While we cannot reinvent history, we can ensure we do better in the future. (NSN 2010e)

This last statement raises a number of questions, which, if nothing else, could help clarify the reality behind such business affairs and prepare the ground for tighter regulation within the industry at large. An interesting detail in the company's latest statement was its defence of the contemporary importance of online filters around the world:

While it is easy to say that there should be no filtering of any kind, we do not believe that would be a wise policy. The fact is that filtering technology is deployed in many, many countries, by many, many operators, for very legitimate purposes . . . On the other hand, there is filtering that we believe is inappropriate and would be inconsistent with widely accepted human rights . . . It is not inconceivable that filtering could be used for purposes such as blocking messages designed to coordinate the assembly of people in order to engage in legitimate political discourse. (NSN 2010e)

This statement indicates that NSN executives were aware of the company's contribution to what they deemed, at best, to be 'legitimate' internet filtering in Iran. But their interpretation of local and regional laws abroad should not be seen as the benchmark for ethical behaviour when their practices and decisions could potentially endanger many civilian lives. In the absence of carefully and consistently enforced regulations, big businesses will continue to find new justifications for dodging voluntary limitations. While NSN officials may be correct that filtering software aimed at fighting online 'crimes' in Western democracies is legitimately produced and marketed, there is still a critical need for concrete, dynamic trade regulations capable of going beyond such a set definition of 'online crime.' When an authoritarian state is incapable of producing the innovative technologies it believes it needs to maintain control, due to a lack of democratic structures in its NIS, the political elite of such a regime will resort to foreign know-how. This will be done under seemingly legitimate covers, which may be followed up by 'upgrade' requests in return for hard-to-refuse sums of oil and gas dollars—enough to persuade any ethical business to suspend its values for a short period of time. If the European Parliament—a largely democratic institution—gives precedence to self-regulation over compulsory directives, then outrageous comments such as the following will be par for the course in the ICT industry:

Consider the fact that the systems that we provided to Iran were designed to implement a right that the ITU has explicitly said is held by member states, and . . . required by law in the vast majority of those member states. Yet, when we help to meet those requirements, we are subject to considerable criticism, including in the European Parliament resolution on Iran of 10 February 2010. (NSN 2010e)

Another issue that is often overlooked when it comes to Western corporations' international trade in ICTs is an East/West divide over the 'ultimate' definition of human rights. Given the history of civil rights abuse in many underdeveloped/developing countries, it is too convenient, yet also too naive, to presume that the contracting regime would be just as repressive without the technology it purchases. Nonetheless this sort of reasoning is implicit in NSN's actions, as is clear from the following statement:

We believe that there is a broad consensus that telecommunications technology and the sharing of ideas and information that it enables, is a tool for social good. Thus, we do not believe that an absolutist policy entailing steps such as a full market exit in the face of evidence of human rights infringements would be a wise approach. (NSN 2010e)

Techno-utopianism for ICTs in general seems particularly misplaced when a company is trying to wipe its hands of culpability for selling specific technologies designed to enable censorship and surveillance. Further, this blasé approach to the contextual impact of ICTs is especially callous when, according to The Economist's (2010) Human Rights Index, Iran ranks 158 out of the 167 assessed countries—tying for eighth worst in the world with Libya, and achieving the dubious honour of ranking third worst in the Middle-East.

The predominantly techno-utopian view in some Western industrial circles ignores the dark sides of the internet, yet seems to be the best case scenario here. To tackle the issue, it would be necessary for ICT firms, their shareholders and their insurers to independently investigate prospective markets in advance and further revise their knowledge following every major political turmoil. This would help them avoid any accidental contributions to online censorship. Although, from a business perspective, one cannot be entirely unsympathetic with NSN's reluctance to pursue a sudden, total market exit after any minor sign of human rights abuse by contracting regimes, nonetheless, it is extremely important for Western ICT companies to understand the political impacts of technology in their target markets. At minimum, they should steer clear of solving 'technical' problems in repressive countries, without first carefully evaluating the 'social' context and consequences.

Self-regulatory measures cannot replace external scrutiny. Frequently revised legislation combined with a standing regulatory task force, democratically elected from within industry, with the specific duty of regulating ICT exports would be an ideal remedy. One of the major socio-political factors influencing the legitimacy of ICT exports, as rightly recognised by NSN, is the human rights environment in a particular country during the lifespan of the foreign contracts (NSN 2010e). Yet NSN's business with Ahmadinejad's neo-conservative government was a simple result of a long-term collaboration started years before at the time of a more reformist government, many of whose officials fell victim to the very same technology they had commissioned.

On a technical level, Deibert and Rohozinski (2010) warn the international human rights community about new, harder-to-detect techniques of internet filtering already being implemented in repressive countries like Iran. These new methods allow authoritarian regimes to continue to control of the nationwide flow of online information while minimising negative external political side-effects of systematic censorship, such as foreign pressure. Referred to by Deibert and Rohozinski as techniques capable of "disabling or attacking critical information assets at key moments in time," they include hardware tinkering, such as shutting off power to the buildings where servers are located as well as software manipulations like tampering with domain name registration. Such methods enable authorities to deny accusations of illegitimate filtering. "In regions where internet connectivity can be spotty, just-in-time blocking is easily reasoned away as just another technical glitch with the internet," they further elaborate, warning researchers that modern internet censorship techniques are not limited to technological methods. With a firm sense of the dynamics of online censorship in repressive countries, they point to "the broad use of slander, libel and other laws to restrict permissible communications and to create a climate of fear, intimidation and ultimately self-censorship . . . [which] reflects a tactic of strangulation, whereby threats of legal action" go a long way in preventing cyber-activists from accessing and posting 'politically sensitive' content.

Anti-Censorship Technology: Fostering Democracy in a Converging World

The protests in Iran since 2009 seem to have shown many Western governments, especially the Obama administration, that current technological sanctions on Iran may be dysfunctional and contradict the original aim of the legislators. Some of Iran's local cyber-activists were doubly disadvantaged by being blacklisted by major American providers of instant messaging, email and social networking services, a few of which were not even blocked by the Iranian regime. Recognising this, the United States government was proactive and undertook a number of helpful steps, ranging from unblocking Iranian citizens on those online services to funding effective anti-filtering software projects. These efforts were intended to foster democracy through facilitating political communication among local cyber-activists and reconnect local cyber-activists to the outside world.

Such actions were widely supported by many scholars, including Nye (2010: 6), who believes the United States government's investment in anti-censorship technology in the aftermath of the 2009 crisis was a wholly legitimate "investment in physical resources that create Soft Power"—a concept he originally developed. Baker (2010) points at many distinct examples where Western intervention has helped promote Soft Power in repressive environments, highlighting the United States Senate's Victims of Iranian Censorship Act passed in July 2009 as part of the Defence Authorisation Bill. This act permits the American government to develop means of circumventing online censorship on behalf of Iranian cyber-activists.

Another prominent example of such efforts by the United States government is the Iranian Digital Empowerment Act passed in December 2009, which allows the export of "software and related services that enable personal communication or allow citizens to bypass government censorship" to Iran. The US State Department also issued a report to the US Congress suggesting that sanctions on "mass-market software for personal internet-based communications" should be waived in Iran's case. Leberknight et al. (2010) explain that the regime's crackdown on cyber-activists following the 2009 presidential election persuaded the US government to make Iran's netizens a foreign policy priority. They also report a list of

related acts that US lawmakers passed between 2002 and 2010, as well as their technological outcomes.

As seen below, the United States government has paid particularly careful attention to the anti-censorship needs of oppressed nations, yielding the creation and release of many effective software solutions over the past decade:

United States Congress and Anti-Censorship Technologies

US Congress Policy	Year	Software Release
Global Internet Freedom Act	2002	Anonymiser Anonymous Surfing, Ultrasurf, Dynaweb
Global Internet Freedom Act	2003	Circumventor
Global Internet Freedom Act	2006	GPass, Firephoenix, Psiphon, Twitter
Global Internet Freedom Act	2007	JAP, GTunnel
Global Internet Freedom Act	2010	Anonymiser Universal, Xi Xang Project (China)

Table 19 (Leberknight et al. 2010)

Yet it is not fair to imply that all the anti-censorship software developed in the United States for use in repressive contexts was initiated by the Senate or the Congress.

Widely popular among Iranian cyber-activists for its effectiveness, speed and relative security, Haystack is a programme that was developed by the San Francisco-based non-profit Censorship Research Centre (CRC) directly response to the Iranian regime's crackdown on the post-election protests in June 2009. According to Heap (2010), the developer behind the project, it "uses a sophisticated mathematical formula to hide the users' real internet identity while allowing them to access websites blocked by Iran's government."

Many other anti-filtering software projects were developed by single individuals—free speech advocates who are skilled coders and mostly reside in North America. In an interview with Shift.com (cited by Patterson and Smith 2005: 41), a well-known Canadian hacker, the founder and executive director of Hacktivism known as Oxblood Ruffin, said he had developed "an anonymous tunnelling protocol program and a program to embed messages inside of gif images to bypass censorship filters," both of which he claims are being widely used in Iran.

It remains unknown whether there is any major anti-filtering software wholly developed by local or expatriate Iranian cyber-activists, although there are at least two potential candidates within this category: Simurgh and Green Proxy. Denning (2007: 26) reports that she and her team of postgraduate researchers "did not find evidence of Iranians developing their own anti-censorship software." Denning's extensive contributions to the state of knowledge on the forms of online activism in repressive contexts are particularly noteworthy, given her reputation as a highly experienced scholar in the field.

Leberknight et al. (2010) list thirteen distinct anti-censorship technologies utilised by software developers, each designed to fit a certain context, depending on project budgets and technological needs, as well as the types of censorship technology that are to be countered:

Common Ways to Bypass Internet Censorship

No.	Anti-censorship Technology
1	Alternative DNS servers/names
2	Open Proxy
3	Hopping IP servers and using popular servers
4	Chopping up content across packet boundaries
5	Concealing payload content by stegano/crypto methods
6	Foundation code, network code, spreading code
7	Change keywords with randomised chain reaction
8	Social media
9	Secure cloud computing
10	Remote login to another computer
11	Secure phase for pre-agreement of protocol
12	Timing covert channels
13	Extensive caching/translation

Table 20 (Leberknight et al. 2010)

Given that most of the above methods are useful in Western, developed countries where censorship is enacted only to a mild degree, many of these techniques can be easily filtered by a well-equipped repressive regime concerned with the rapid growth of cyber-activism. Much of the software aimed at people residing in states such as Iran and China relies on the first three technologies indicated on the above table. A Freedom House (2011) report lists the major anti-filtering software products commonly used by local Iranian cyber-activists, evaluating them based on the ease of use, practical effectiveness and security features, and scoring them on an overall basis:

Anti-Censorship Software: A Comparative Evaluation

No.	Software	Ease of Use	Performance	Support and Security	Overall Score
1	Dynaweb	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
2	Freerate	★ ★ ★ ★	★ ★ ★	★ ★	★ ★ ★
3	Freenet	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
4	GTunnel	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
5	Google	★ ★ ★ ★	★ ★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
6	GPass	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
7	Hotspot Shield	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
8	JAP	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
9	Proxies	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
10	Psiphon	★ ★ ★	★ ★ ★	★ ★	★ ★ ★
11	TOR	★ ★ ★	★ ★ ★	★ ★ ★	★ ★ ★
12	UltraSurf	★ ★ ★ ★	★ ★ ★	★ ★ ★	★ ★ ★
13	Your Freedom	★ ★ ★	★ ★ ★ ★	★ ★ ★	★ ★ ★
14	VPNs	★ ★ ★ ★	★ ★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

Table 21 (Freedom House 2011)

The majority of the software listed above was developed in the United States and Canada, where many influential philanthropic organisations are headquartered and where nearly half of the Iranian expatriate community resides. VPNs, as confirmed in a number of the expert interviews, were the seen to be the most popular and effective anti-censorship tools among local cyber-activists. Freedom House analyses such 'solutions,' mapping them out according to their technical capacities and the socio-political contexts they might best serve. These software products were assessed based on download and upload speeds, as well as the levels of privacy and security they provide their users:

Anti-censorship Technologies: One Size Does Not Fit All

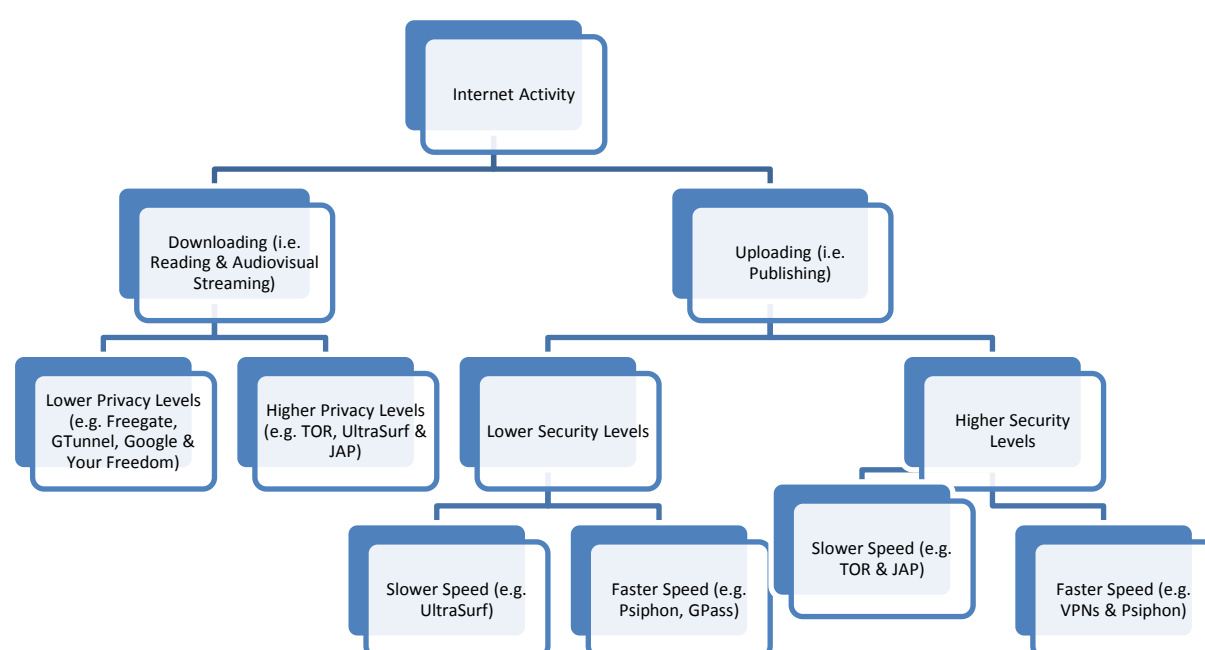


Figure 35 (ibid)

As indicated in the above figure, UltraSurf, Psiphon and VPNs are the most efficient software products in their respective categories. What distinguishes them from numerous, less successful competitors seems largely to be the sophisticated, innovative technology they rely on. According to Roberts et al. (2009, cited by Shahab and Mousoli 2010: 10), tools such as Tor, JAP and Circumventor rely merely on peer-to-peer technology to enable cyber-activists to use their own computers as proxies to tackle blocking, while UltraSurf relies on "sophisticated anti-blocking technologies to outwit filterers. Because very few people use a given Psiphon node, it is less likely to be blocked."

Given that the interviewees were chosen from across a range of no fewer than three distinct professional categories (e.g. academic, practitioner, and activist), they did in many key cases disagree with one another. In fact, the fundamental challenge arising from the interviewing process was not the design of a 'perfect' questionnaire, but the ability to arrive at sociologically meaningful conclusions. Regarding the analysis of the interview scripts, a set of criteria (see chapter iii) comprising mainly of the interviewees' background and accomplishments was implemented to determine the credibility of every interviewee's answer.

Hactivism and Innovation: The Blurred Lines of Online Dissent

The use of technological innovations by Iranian cyber-activists has never been limited to the passive use of anti-filtering software. Over the past decade there have been many credible reports of politically motivated hacking attacks against the regime's online propaganda arms, carried out from inside and outside the country mostly by anonymous, professional Iranian hackers. Certain verified, original, high-tech, 'zero-day' operations have been accompanied by hundreds of minor attacks carried out by more ordinary, less technically literate cyber-activists.

These smaller attacks tend to take the form of the Distributed Denial of Service (DDoS) attack and often employ pre-made, user-friendly hacking software, referred to by Knapp and Boulton (2006: 79) as "downloadable and graphic-interfaced tools," such as pagerboot.com. DDoS attacks are described as based on dynamic HTML templates to launch 'HTTP floods'—making a given website temporarily unavailable via unusually excessive viewing demand. Such attacks are especially popular in developing countries, "where networks and infrastructure tend to be fragile and prone to disruption" (Deibert and Rohozinski 2010: 4). Asghari (2010: 18) has seen evidence of DDoS attacks escalating dramatically during the two weeks following Iran's disputed presidential election in 2009, arguing that these attacks were mostly directed towards "government-run news and media sites, as both a form of protest and to stop propaganda." He also stresses that these attacks were carried out from both inside and outside the country, with outsiders making up most of the participants, especially Iranian cyber-activists residing in the United States and Europe. Hearn et al. (2009: 3), similarly acknowledge that most DDoS attacks against Iranian sites were launched from "Western countries and in particular the United States of America." Rathmell (cited by Stohl 2007: 14) also verifies that exiled political opposition groups exploited Iran's online sphere, counting four main strategies deployed: "virtual sit-ins and blockades; automated e-mail bombs; web hacks and computer break-ins; and computer viruses and worms." Nazario (2009: 171), a senior security research manager at Arbor Networks, reported that his organisation's network recorded multiple signs of collective-organised mass DDoS attacks on Iran's governmental websites following the 2009 disputed presidential election, many of which were coordinated on popular social networks such as Twitter and Facebook. Yet the "attackers just as quickly suggested the attacks stop due to bandwidth consumption issues in light of the country's internet traffic filtering. It is unclear if the attacks had any significant impact on the target sites' availability." The following snapshot of a Twitter update posted by an anonymous Iranian cyber-activist shortly after the 2009 election invites the individual's 'followers' to join them for a DDoS attack against a selection of regime-run websites:

Twitter: DDoS Attacks Go Viral



Figure 36 (Wired 2009)

Based on this information, one could hazard that what was initially perceived by the international media to be the regime pulling the plug on the internet was, in fact, a direct side-effect of Iranian cyber-activists clogging the country's very limited bandwidth through excessive traffic. If so, this would have mainly been due to Iran's centralised, state-controlled and deliberately incapacitated network infrastructure, which would not have been able to keep up with the development of the events. This means that if DDoS attacks are used as viral practice, they can cause just as much trouble for home web users as for government employees, by disrupting shared connections and eventually bringing services to a temporary standstill. This result would arguably favour the regime more than cyber-activists looking to the internet as a last resort to coordinate their activities 'in time' and to get first-hand news out of the country despite the ban on foreign media organisations. While Nazario chalks up the popularity of DDoS attacks amongst Iranian cyber-activists to their ease of use for non-technical parties, Deibert and Rohozinski (2007: 34) believe that the effectiveness and relative security of such operations also play a role in their widespread employment. They assert that a DDoS attack is "particularly effective as [it] can occur anonymously, with no demands being made, and presents investigators with the difficult task of pinpointing the source of the attack." Yet they may be overlooking the fact that user-friendliness and safety are only valuable features as long as the network is up and running, and that if these techniques may shoot cyber-activists in the foot by disrupting internet service in general, cutting the flow of information, then they are ultimately serving the regime's censorship policies.

This raises the question of whether Iranian cyber-activists are the only parties in Iran's online power struggles that employ hacking attacks. The Iranian regime has a history of launching advanced hacking attacks against both local and expatriate cyber-activists, as well as foreign governments. The exact scope of Iran's cyber-strength remains unknown due to inconsistencies of the available reports. Valeriano and Maness (2012: 147) found that while Iran had a considerable amount of control on the internet, its cyber-power was not as dominant as that of United States, Russia, China and Israel, concluding that "Iran falls somewhere on the lower end scale in that it has very little offensive capabilities but is also

less dependent overall and remains in control of access points." The following table demonstrates Iran's overall position as compared to the world's top four cyber powers:

World's Top Cyber Powers under Scrutiny

Country	Cyber Offensive Power	Cyber Dependence	Cyber Defensive Power	Total Score
Iran	4	5	3	12
USA	8	2	4	14
Israel	8	3	4	15
China	5	4	6	15
Russia	7	5	4	16

Table 22 (American Foreign Policy Council 2012; Ganji et al. 2013; Hastedt et al. 2014; Strinde 2011)

If they can be relied on, these numbers suggest that the Islamic Republic's cyber-activities are designed largely for defence—meaning that despite having a relatively good ability to detect and stop incoming cyber-attacks, the regime's ability to break through the sophisticated firewalls of industrial states remains below average at best. The table also confirms that the country depends heavily on foreign-sourced technology and infrastructure with regards to the internet. While the regime's online intelligence unit may have conducted international operations, it has rarely hesitated to hack the websites and blogs of local cyber-activists and even many reformist political figures. This is cheaper, more effective and less politically fraught than publicly acknowledging that dissident voices are not tolerated. Patterson and Smith (2005: 42) found that the blog of Mohammad Abtahi, the former Iranian Vice President, "was hacked numerous times in response to his postings regarding the government torture of other bloggers." They report that the official website of ex-Presidential candidate Ali Larijani's was also hacked: "the attacks on the websites of Larijani and Abtahi indicate that elements within the country are attempting to silence the opposition." Deibert and Rohozinski (2010: 1) also confirm that Iranian authorities are no longer limiting themselves to pursuing old, passive-defensive filtering methods and "are taking active counter-measures aimed at controlling the spaces online for resistance and dissent."

Whether the Iranian regime centrally controls the execution of attacks or contracts them out to professional hacker groups remains a question, as there is no substantial public evidence available on the issue. There seem to be enough indicators, however, to suggest that the situation is a hybrid one. Denning (2007: 27) argues that Iran has a large community of online security experts and scholars, including many who would be suitable for the job. She estimates "that there are 100 or more academics working in information security, publishing research papers in journals and conference proceedings, hosting and attending conferences, and teaching courses on network security topics." Yet it would be premature to draw any conclusions before assessing the background and political tendency of each and every one of those academics. Interestingly enough, Denning claims to have found evidence of "research in network security taking place within government labs," which cannot on its own be taken as a proof of hacking activity. Patterson and Smith (2005: 19) are certain that a large proportion of network security research in Iran takes place at the Sharif University of Technology, but they acknowledge that they found "no evidence that the school was using this education to promote hacking in any way."

It is important to note that not all professional hackers who cooperate with security officials in such projects are financially driven, and that the regime can always find enough

conservative and religious academics to rely on, provided that they can make a convincing case for the 'harmfulness' of the voices to be silenced. Patterson and Smith (2005) say they have found substantial evidence of such politically and religiously motivated hacking attacks taking place in Iran.

In conclusion, increasingly the argument over the democratic or repressive nature of the internet comes across as vain. Web 2.0 technologies are highly dynamic and the leverage that any party to Iran's power struggles can gain by using them cannot be taken for granted. Winning such exhausting and time-sensitive engagements takes persistence in remaining on top of the innovation pyramid—any anti-censorship innovation can and inevitably will, at some point, turn into just another abandoned, worthless piece of software, if not regularly evaluated and updated. The failure to acknowledge that online innovations are not 'timeless' is the main reason why technologically deterministic solutions to cyber-censorship introduced by the West have so far resulted only in the production of a handful of software products that intended clients 'used to' find useful at best. This outlook concurs with Deibert and Rohozinski (2010: 2) when they state that "not that long ago it would have been safe to assume the entrenched authorities were at a disadvantage, too inept to withstand digitally-enabled social movements. Today, that is no longer a safe assumption." Whenever a brand new means of communication appears, history has shown us that efforts at censorship will eventually follow in due course. Drezner (2010: 41), however, insists that the long-term benefits of the internet and online technologies will fall to the favour of cyber-activists who can exploit them to damage authoritarian regimes, asserting that "over time, authoritarian governments will be faced with a difficult choice: accept a greater risk of popular revolt, or engage in costly acts of repression." From an SST perspective, the validity of Drezner's viewpoint on the long-term benefits of the internet for cyber-activism would depend strictly on his concept of 'exploitation'. Nevertheless, the latter part of the author's argument is too techno-utopian to fit the contextual realities of modern Iran. As we know, the Iranian regime manages to balance online censorship and crackdowns on street protests—it has hardly shown any real sign of weakening despite extensive international pressure. An online movement can only be sustained in the context of a democratic, functional innovation system, capable of the timely creation and diffusion of unique technologies, determined by immediate needs and truly bottom-up processes. Where this is not possible, as is the case in Iran, ICT imports can go a long way to fill in gaps—for either side of a conflict.

The main conclusions of the study at hand follow in the next chapter.

Chapter vii: Conclusions, Practical Implications and Insights for Future Research

The seventh and last chapter of this thesis comprises a thorough account of the conclusions drawn based on previous chapters and how they were arrived at, as well as providing experiential insights for future studies of similar nature.

The results of this research chiefly confirm that Iran's NIS is bimodal. This bimodality is entrenched in the Islamic Republic's preoccupation with militaristic and ideological objectives, such as its nuclear programme. The divisions in this unconventional form of NIS, fall along the lines of the online power struggle in Iran—an ICT-mediated conflict between pro-democracy cyber-activists and actors employed by the ruling elite or who support it ideologically. The Iranian system stands in great contrast to Freeman and Lundvall's classic model of nationwide innovation processes, where academia, governmental institutions and business enterprises interact efficiently to serve national and at times international interests, rather than merely achieving pre-set technological goals championed by unelected officials in control of a political regime largely characterised by what Habermas (1989: 19) refers to as "personalised state authority." This illegitimate model of governance seems to take advantage of the Platonic-Aristotelian (Arendt 1961: 105) valid principle that "every well-ordered community is constituted of those who rule and those who are ruled."

Outright Bimodality vs. Limited Diffusion: Can A Single NIS Serve Two Different Masters?

The bimodality of Iran's system is not unique, but it is profoundly significant to the social diffusion of technological innovations. A thorough assessment of the IRGC's influence on the country's ICT industry shows that the civil sector's contributions to nationwide innovation processes in the field are marginal at best. This effect is hardly surprising in an undemocratic political system that exerts a firm hand on the national economy. Yet bimodality is not specific to the underdeveloped world. Perhaps the most notable contemporary example of a bimodal NIS is found in the United States. Beduya (2009) argues that two completely separate modes are at work in the National Innovation System of the United States, both of which are based on free-market capitalism: "one component that is founded on Eisenhower's so called military-industrial complex has already yielded such gems like the Internet and the GPS. The other part, mainly for downstream applications and commercial diffusion, is the linked University and venture capital firms that is, for example, the foundation of Silicon Valley." Despite this bimodality, there is no evidence to suggest that the NIS of the United State is weak or dysfunctional. But a large question remains regarding how genuinely democratic the US political structure is, when compared to that of the Scandinavian states, home of the NIS theory as we know it today. This line of inquiry is thoroughly underexplored and in need of much further scrutiny.

In the case of Iran, the dominant, governmental part of the system is run by core regime officials mostly located within the IRGC and directly supervised by the Supreme Leader. The IRGC, furthermore, has a tendency to employ seemingly private front companies in order to achieve two goals: outcompeting its private sector rivals in profitable national projects without provoking criticism, and circumventing international economic sanctions by attempting to deceive Western companies into contributing to projects presented as having civil purposes.

The alternative, pro-democracy faction of the NIS structure under study, meanwhile, is largely civil, and thus has access to a much smaller budget. Consisting of an interconnected, virally active network of local and expatriate Iranian cyber-activists, this portion of the NIS empirically represents a much larger, as well as demographically more diverse, section of the population. Concentrated in the civilian universities and research firms, or performing as individual operators, these actors are deprived of any major share of the national research and development budget, while also being regularly subjected to thorough surveillance and occasionally to interrogation, arrest and criminal prosecution.

These two sections of the Iranian NIS are political foes—hence the bimodality. With both sides' increasing reliance on ICTs due to digital globalisation, the secular forces' four-decade-long power struggle against the Islamic Republic has largely shifted into the online sphere since early to mid-2000s and away from traditional, physical methods. This has resulted in the formation of a phenomenon known as the Persian online discourse, which consists predominantly of, but is not synonymous to, the Persian blogosphere—home of Iranian cyber-activists worldwide.

The weblog sampling process was indeed a challenging one, posing a fundamental dilemma on whether or not the research should directly engage with the cyber-activists under scrutiny. While the initial inclination was to cross the boundaries of conventional trends, this preliminary strategy was later on dismissed following further supervisory consultancy, as well as on various ethical grounds. All things considered, the ultimate verdict was that even in the case of penetrating the technical barriers, there would have been no feasible way of measuring up the validity of data at least from a purely academic stance. Also, among the main factors compromising the pace and robustness of the research were: the frequent discontinuation of many weblogs, the technical incompetency of some bloggers who would otherwise be more vocal, the IRGC's occasional blanket disruptions of the blogging platforms at key political flashpoints, and of course the highly challenging issue of data authentication.

While the weblogs discontinued in the early stages of data collection were automatically eliminated from the list, those doing so further down into the process were often considered to be kept in the loop. With regards to the blocked weblogs, it happened often that the blogger swiftly informed their core audience about their involuntary relocation through their fellow activist bloggers likely to share the same core audience, who were able to widely circulate the URL to their new homepage. At the time of government-imposed blackouts, however, the research was left virtually paralysed, as such episodes made it almost impossible to receive any live updates from the local cyber-activists for indefinite lengths of time and at the point they were most desperately needed.

Despite the fact that Iran is the highest ranking country in the Middle-East in terms of web connectivity, it is vital to note that broadband internet remains a luxury afforded almost exclusively by those in more affluent urban areas, as is the case with most emerging economies. A distinctive characteristic of social sciences is the liberating ability to move beyond oversimplified notions such as the inevitable divide between the information 'haves' and 'have-nots'. But from a socially constructivist perspective (i.e. STS), issues such as access remain to be the cornerstone of a dynamic research design involving bottom-up social processes. For instance, few of the active anti-censorship bloggers studied by this project were based in Iran, whereas even more ICT fluent political activists than initially expected were expatriates. Such so-called resource-specific split proved during the course of the

research to be largely intact, however, between the native and expatriate cyber-activists, rather than the rich and the poor.

IRGC Generals and the Militarisation of Iran's Civil Industries: The Birth of A Dysfunctional System

For over a decade, since its recognition of the online sphere as penetrating and influential, the regime has made systematic, costly attempts to take control of political discourse therein. Yet it has had very little luck, largely due to the existence of a separate, parallel innovation system maintained by a tangled web of young, educated cyber-activists who, despite political isolation and resource deprivation, remain relatively competitive in an online struggle with the regime.

This research verifies that the Iranian NIS is dysfunctional. The results also demonstrate that Western, mainly European, telecommunications companies have continuously influenced the country's political discourse by filling its growing technological void. They have extensive input into the online power struggles in Iran by engaging in questionable business transactions and contracts with the Islamic regime.

Furthermore, the research finds a largely set pattern in the way Western corporations have contributed to the telecommunications technologies industry in Iran. While the list of the actors supplying the regime's needs consists, predominantly, of north-western European ICT companies, for the most part cyber-activists tend to rely on North American universities, strategic research centres, and philanthropic NGOs. An analytical comparison indicates that foreign contributions to the efforts of the Islamic Republic are merely profit-driven, whereas technological assistance aimed at cyber-activists is primarily humanitarian. I argue that the geographical basis of this distinctive division is a matter of policy.

Transnational conglomerates have often been singled out by human rights organisations for their involvement in certain markets. The instance most relevant to this study is the lawsuit filed in the United States District Court for the Eastern District of Virginia against Nokia-Siemens Networks by Iranian cyber-activists in the aftermath of the contested 2009 presidential elections, in which the company was accused of providing the Iranian regime with online censorship technology. NSN is only one of many European corporations that have successfully plead ignorance of their contractual partners' repressive use of what such companies perceive to be peaceful, lawfully justifiable technology. Yet there is a world of difference between European and Asian legal systems with regards to conceptions of 'criminality'—yielding a clash of ethics. A well-rounded policy would be one that carefully takes into account not merely what importing countries' regulations dictate, but more importantly inscribes codes of conduct based on liberal, European principles. That is the only way the European Union can ensure the success of profitable businesses while not at the same time disfavours 'the oppressed.'

The focus of a practical, dynamic policy must be twofold: it needs to effectively prevent the sale of sensitive, dual-purpose ICTs to repressive regimes, and further facilitate pro-democracy movements' access to telecommunications technologies useful in countering repression as well as to resources to bolster their ability to innovate in the field. Currently, many policies in the European export control regime remain static and underdeveloped. They hardly ever keep pace with technological advances in ICT, and often result from technical perspectives that target entire systems, rather than recognising, evaluating and dynamically

engaging with the various socio-political elements at work within that system. There is a burgeoning need for the West's export policies to become more goal-oriented, more contextually informed and more socio-technically balanced. Currently they seem more or less like diplomatic gestures aiming to demonstrate to oppressive regimes that they are not scientifically self-sufficient. The dysfunctions of a repressive regime need to be seen primarily by the international community as a long-term threat to the welfare of its citizens, not as a profiting opportunity. Any other approach would not be consistent with codes and principles of corporate social responsibility.

The dysfunctional nature of the Iranian NIS is not automatically caused by its bimodality, but rather by the undemocratic structure of its political system. There have been multiple instances where a country with a bimodal NIS has not become overly dependent on foreign technology imports. Among these is Norway, where according to a report authored by Herstad et al. (2011: 14), a dual NIS is in action: "the large capital region proportion of industrial activity collectively forms a context of dense internal buzz from face-to-face contact and individual knowledge worker mobility . . . [whereas] firms in other Norwegian regions link up with and contribute to the construction of . . . domestic innovation collaboration networks." Characterised by diversity (Wicken 2007), Norway has one of the most successful National Innovation Systems in Europe and in the world (Haghi et al. 2011).

While a bimodal NIS can, occasionally, remain functional, the malfunctions of the Iranian system result not necessarily from the state versus civilian division it faces nationwide, but rather chiefly from its socio-political divide into factions—itself an undemocratic, military-oriented social construction. This brings to mind the dependency of the United States defence industry on Japanese technologies made for civil purposes towards the end of the 20th century (Alvarez 1989, cited by Institute for International Economics 2006a). At one point, only one third of the products using semiconductors in the United States were made in the heart of the industry in California (Irwin 1996)—the Pentagon relied increasingly on commercially-purposed Japanese products for convenience. But as a New York Times (1991) special report rightly pointed out at the time, "the spinoffs are now going the other way: A healthy commercial industry is considered necessary for the military." This observation is essential to understanding the political rhetoric behind innovation choices. The biggest consequence of this pattern—an unorthodox drift from Freeman and Lundvall's original NIS model—was, according to the aforementioned report, "that the United States, lacking a consumer electronics business and behind in production of certain types of semiconductors, [became] dependent on Japan and other nations for technology used in weapons." This is why scholarly arguments that rule out the potential power of the European Union to pressure the Islamic Republic are unconvincing. With Iran being thoroughly dependent on European ICTs, the EU is economically best placed to help make a major policy shift happen with regards to Iran (Ganor 1998).

Why Democracy Matters: The Social Structure of an NIS and Its Technical Potency

The absence of democratic NIS structure in Iran is not fundamentally dissimilar to the situation in the United States immediately after World War II—military-focused and divided. This study establishes that Iran's NIS is undemocratic in terms of both socio-political representation and gender distribution. It found that gender and location were both influential on the computer-literacy and connectivity of politically motivated Iranian cyber-activists, but did not significantly affect their innovativeness. Recent statistics show that the nation's

household internet connections are almost equally shared between male and female users across the entire population. Therefore, the undemocratic nature of Iran's NIS seems to be due to the lack of democracy and gender equality that both the pro-regime and cyber-activist factions display. Again, only one of the assessed activist blogs was definitely maintained by a woman.

As a final conclusion, it is hardly an accident that Ukrainian cyber-activists were mostly passive consumers of ICTs, as opposed to prolific innovators, at the time of the Orange Revolution. According to Transparency International (2011), "corruption in Ukraine is a systemic problem existing across the board and at all levels of public administration." In a country where there is tolerance for state corruption—a blatant sign of a lack of democratic structures—the NIS is inevitably distorted away from Freeman and Lundvall's natural model. The socio-technical similarities shared by the Iranian and Ukrainian case studies could be developed as an analytical dimension useful for future research on the interplay between state politics and NIS functionality in repressive environments. This would be particularly beneficial to Western policy-makers in their attempts to move away from symbolic standoffs towards practical anti-censorship solutions, in turn enabling democratic social movements in dictatorial states.

Ukraine of the mid-2000s may not have had many significant cultural values in common with Iran later in the decade—a considerably more restricted nation in almost every aspect of social life. But when it comes to its NIS dynamics and processes, the resemblance is uncanny. The lack of systematic democratic assessment and consequently the absence of an adequate policy reform regimen in relation to repressive countries have both historically restricted the West's ability to fully utilise its vast potential to facilitate democratisation processes in emerging economies—demonstrated yet again during the Arab Spring protests. The best solution to this shortcoming, as this research has argued throughout, is a legislative one. The proposed framework stands in contrast to one-size-fits-all schemes that often do not reach far beyond symbols and metaphors. Without flexible, contextually informed and frequently revised policies advancing democratic political reform in repressive countries, nationwide innovation in such countries will remain distorted. This is a lost opportunity for the global promotion of democracy. The free world must step up its strategy to go all the way from disapproving of repressive conduct to discontinuing technological cooperation with non-democratic elites worldwide.

The Orange Revolution in Ukraine has more or less the same social goals and values in common with most other political movements of its time: civil liberties, financial stability and a minimal, transparent government. Ironically, it also shares the same roadmap with them: none. Contemporary popular uprisings and their international supporters often tend to be too focused on toppling oppressive regimes to pay enough attention to sociologically justifying the long-term impacts of their actions and strategies on worldwide stability and peace. The Orange Revolution was one of the first scalable attempts at the idea of a Western-backed, colour-coded and non-violent political resistance movement against a totalitarian regime in the modern history of civil disobedience. Yet the departure of the dictator left behind a familiar phenomenon in all layers of the society's fabric, one we could refer to as the 'culture of corruption'. This, along with the inexperience of the opposition, caused by years of regime monopoly across the political scene, is exactly why not many of those residing in the Arab Spring states can yet claim to be living in better conditions than they did prior to the power shift in their respective countries. The mere transition of control from one party to another, without activating a set of democratic safeguards to preserve minority rights

(including those of supporters of the prior regime) simply leads to what has been witnessed in Iraq, Tunisia, Egypt and Libya. In Egypt, for instance, the same censorship technology that served President Mubarak was used by Muslim Brotherhood officials to control the internet, despite a fundamental regime change—a scenario all too familiar for those carefully following the aftermath of recent regime changes in other parts of the region.

In Ukraine's case, the underdevelopment of counter-censorship activities was less deeply rooted in a lack of resources than in the defectiveness of its security-focused innovation system—a legacy inherited from Soviet Russia. This familiar pattern confirms that it is mostly human choices rather than newly emergent technologies themselves that ultimately define sophisticated technological concepts like usefulness and impact. If the sheer existence of a technical innovation could be sufficient to promote a major cause, then the phenomenon commonly referred to in the media as a 'Facebook/Twitter revolution' would have ultimately coincided with relatively higher levels of democracy in the associated countries. But instead, what happened in almost every case was the transfer of censorship technologies from one oppressive hand to another. The International Renaissance Foundation and Stefan Batory Foundation (2010: 63) reported over five years after the Orange Revolution that Ukrainian innovation processes are idle, explaining that "although the market economy has been de-facto established in Ukraine . . . the manageability and efficiency of . . . innovation[s] is highly questionable . . . Several cases of re-privatisation motivated by non-transparent privatisation procedures have created uncertainties diverting potential investors."

This is not to suggest that Ukraine performs inadequately in the academic sector, but to highlight the defective system through which Ukrainian universities interact with the government and major industries. According to Outsourcing Centre (2005), in the mid-2000s the country benefited from nearly one thousand colleges and six hundred thousand students. In the year of the Orange Revolution the Centre reported that "the National Academy of Sciences, whilst reduced in the course of the 1990s brain drain, employs almost 30,000 engineers and researchers. Today, the Academy supports 170 scientific research institutes, including the internationally renowned Glushkov Institute of Cybernetics, and eight techno-parks which address the challenges of innovation." From an NIS perspective, however, Ukraine ranked 71st out of 142 assessed nations in 2013—stuck around the halfway mark (Global Innovation Index 2013). This is a fairly improved position, given the country's position at the 85th place on the index earlier in 2005 (Blanke 2005). With regards to telecommunications technologies, however, "Ukraine has not been harnessing these new tools for growth, ranking 76th overall on the ICT sub-index" (ibid).

Just like in Iran, dysfunctions in Ukraine's NIS resulting from the repression have widened the technological divide between the government and cyber-activists in favour of the former, once again highlighting the role of democracy and transparency in the construction of a unified, self-reliant innovation system at the national level. Although Ukraine seems to have an abundance of knowledge production firms to address such questions, its research and development funds are not diffused in a 'democratic' manner. It is not a lack of resources, knowledge or ability that makes its NIS relatively incompetent, but rather the notoriously high rates of corruption within Ukraine's political elite. While this led to an inevitable decrease of foreign investment in the Ukrainian market, corruption has not stopped Western companies from seeking business with governmental institutions in Iran and in other parts of the Middle East and North Africa (MENA). This trend is influenced by a range of local and cross-border factors including the affluence of most natural-resource based MENA economies and the fear of another economic recession in the Euro zone, which makes it hard

for struggling EU businesses to refuse attractive deals on offer from repressive states rich in oil and gas. According to Forbes (2013), "Ukraine needs a business climate where agreements are fulfilled, investments are secure, and courts take independent decisions regardless of who the claimants are." If these weaknesses are all resolved, "international investors will flow in, small and medium business will develop, competition will foster innovation and efficiency, and the country will finally be able to fulfil its vast potential" (ibid). Heavy reliance on foreign technologies is never good news for a country's innovation system, and certainly represents a catastrophe for pro-democracy cyber-activists facing systematic governmental censorship. The dependence of the Iranian CIS on ICT imports seems to be a symptom of a dysfunctional NIS. The best, perhaps only, remedy would be a thorough democratic restructuring.

By the same token, unless important democratic values and principles are fostered in Iran, ICT imports will remain generally more beneficial to the dictatorial regime than to pro-democracy dissent. Regarding Ukraine, Salnykova (2006: 28) calls attention to the economic experiment implemented by the parliament from 1999 to 2002 affecting the country's ore-mining and metallurgical enterprises, under which "enterprise profit tax (EPT) was set at the level of 30 per cent of the usual tax (that is only 9 per cent of profit) . . . [and] road funds fees were annulled, the state innovation fund fee was reduced to 50 per cent." Yet the scheme had no durable impact on Ukraine's NIS output. The reason for this failure is that while the Ukrainian parliament—the most democratic institution within the regime—was busy introducing potentially useful tax reforms, the extra-judicial faction of the regime led by Kuchma and Yushchenko engaged in high levels of corruption, conducted mainly via "presidential control over the Prosecutor General's office under both the 1996 and 2006 constitutions" (Kuzio 2008: 4).

Finally, despite receiving extensive Western financial aids, and while encountering a relatively limited scope of governmental censorship, pro-democracy dissidents in Ukraine have remained unable to make full use of the ICTs available to them in the years following the Orange Revolution. The fact that a transition of the country's pro-democracy discourse to the online sphere did not occur in a timely, effective manner could be one reason, among many, for why the Ukrainian protesters are once again struggling—with a now much more technologically experienced government, ironically headed by Viktor Yanukovich, the very same man they successfully defeated in 2005. According to Lutsevych (2013: 7), the Razumkov Centre, a leading Ukrainian think tank, "has 748 followers on Facebook, whereas the Moldovan Foreign Policy Association and the Institute of Public Policy in Chisinau have no Facebook presence at all," elaborating that "even for the most successful groups, the social media dynamic is weak . . . [and] poor media outreach weakens NGOs." Although there seems to be a need for Ukrainian and Moldovan political activists to scale up their 'digitalisation' efforts, the Iranian opposition hardly suffers from computer illiteracy. The official Facebook page of Mohammad Khatami, Iran's former president and a father figure for political reformism in the Islamic Republic, has over 107,000 'likes' and counting—despite the fact that Facebook has been officially blocked in Iran since 2007 (HAMSA) in what is the first known instance of an SNS being systematically filtered in a repressive country.

In Search of a Cross-Border Model for Democratic Change: A Universally Transferrable NIS?

Empirical analysis of NIS in Iranian and Ukrainian cases has inspired this research to seek a fresh, cross-border framework useful to the West's global promotion of democracy. Even though the comparison of the two case studies at hand demonstrates that there is a direct correlation between NIS functionality and the level of democracy found therein, the idea of a collective solution seems a little too optimistic. In other words, although it is suggested here that the way to foster democracy and human rights in a repressive country ought to best pass through embracing legitimate technological needs and interests of pro-democracy dissidents, it remains unclear at this point if a globally applicable remedy could be an option. Yet the universal acceptance of the intellectual advantages of non-deterministic, context-driven approaches would be a positive step towards further progress in this mostly underexplored field.

The idea of an internationally transferable model of a democratic NIS (or any other type of a socio-technical system for that matter) is one "beset by a fuzzy [form of] utopianism" (Warren 1996: 242)—an insight partly rooted in "the false cultural reification of the East by the West . . . or a responsive false cultural reification of the East by its more authoritarian leaders" (Morgan 2006: 97). An NIS can fail for a variety of interdisciplinary reasons. Instead of attempting to faithfully replicate 'successful' models in emerging economies, regardless of their unique characteristics, the West should focus on identifying, explaining and adequately addressing the contextual barriers that prevent a functional, independent NIS from flourishing in repressive countries. This gap in the literature, as Minogue (2001: 7) argues in regards to Western reform packages, creates a distorted scene in which "failures are largely blamed on the recipients . . . [and] successes are seized on and promoted [as] examples of the virtuousness of the donors." This only reinforces a discursive context "increasingly premised on the apparently indispensable precondition of one united, cultural identity and a common language" (Mishkova 2012: 675). Such top-down, idealistic plans have historically proven to be "difficult and costly" (Sofka 2005: 1)—and on many occasions impossible to execute.

If we step away from what is known in some neo-conservative circles as "the requirement for international order" (Porch 2013: 28), we will realise that without the implementation of many crucial prerequisites in emerging economies, such as trust (Fukuyama 1996)—a sophisticated concept "inherent in the Western democratic model" (Secor and O'Loughlin 2005)—an NIS may not be fully transferrable across geographical borders. The abrupt imposition of a complex socio-technical structure from one geographical territory to another will not necessarily successfully transfer the democratic norms and values that it fundamentally relies upon. Further, it is inherently undemocratic to attempt to democratise a sovereign system via top-down influence. Such an approach will ignore the inherent sophistications of existing political institutions, which according to Magone (2006: 103), are "cultural artifacts and . . . are subject to change to adjust to new situations." Technological innovations often best serve the social contexts for which they have been developed, and the chances of a given technology's successful cross-border application remain heavily dependent on a range of factors in the destination country's culture. Democratic progress in repressive states may become a reality if Western powers make a policy shift from attempting to unilaterally decide the pace and direction of change to patiently assisting bottom-up, context-driven processes that will allow true democracy to flourish according to local cultural conditions. Thus, as Mohan (2011: 174) rightfully argues, "Pakistan, Afghanistan, Iraq, Iran,

Kenya, China, and even Russia will adapt to democratic institutions only in harmony with their own national traditions."

This techno-real approach adheres to Weber's (1922) philosophy, which held cross-cultural transfer of institutions to be quite restricted. The reason for this limitation, as Honigsheim (2003: 27) points out, is the accepted "balance established in some countries between bureaucracy and democracy and the attitude of majorities towards minorities." The relatively relaxed political culture currently at work in many parts of the West is not an overnight phenomenon; it clearly derives from a history of bottom-up democratic processes led by those directly benefiting from them. Conversely, the European Union's current approach to the global promotion of democracy tends to be rooted in that put forth by Dahl (2000), who strongly believed in the worldwide transferability of "democratic units". As appealing as such a concept may sound, wishful thinking is not a practical strategy. The EU's multiple attempts at transferring democratic institutions to repressive states have remained predominantly symbolic and contradict some of "the principles formulated [for] the creation of a socio-economic environment favouring democratisation in the respective countries" (Paulsen 2007: 29). Although neither Weber nor Dahl lived in—or perhaps even anticipated—a digitalised world like ours, Weber's insights on the international transferability of institutions seem to be considerably more relevant to the post-internet dynamics of political change than those of Dahl's. Today ICTs facilitate the cross-cultural transferability of innovations "through communications networks and . . . [through increasing] . . . the ability of firms to engage in global production" (Institute for International Economics 2006b). Even so, Weber's scepticism regarding the successful transmission of democratic systems remains highly relevant. Further, as digital globalisation amplifies the influence of foreign actors on a country's innovation output via the blurring of national borders, NIS theory has a critical need to adapt to these realities of the modern world, in order to stay relevant.

The current lack of a universally transferrable model of innovation should not, by any means, be considered a policy dead-end. The West must invest the valuable resources it has into a dual strategy, on one hand developing a competent ICT export regimen, and on the other hand re-theorising its approach to fostering democracy in repressive countries, in part via commissioning relevant scholarly research with better methodological approaches. This will enable EU lawmakers to benefit from an 'action-oriented' mechanism relying simultaneously on recent academic output as well as accurate local knowledge.

Despite its widespread applicability in the industrialised world, the NIS model is inaccurate and insufficient in states where foreign influence is a highly influential factor. GTZ (2008) argues that even if careful attention were paid when applying the NIS model to regional, supra-national contexts, the framework would still lack enough vision and complexity with regard to major channels that may potentially influence innovation processes. GTZ explains that "cross-border transfer of innovations happen through multiple channels—for instance, imports of new products and capital goods, cross-border flows of ideas and information, education abroad, employment of expatriates, [and] advice and support from buyers." In addition, Van Lobbeeght (2012: 25) articulates that "the cross-national transfer of innovations is explained by the extent to which firms in different countries compete with each other in the global economy . . . [and that] codes are more likely to be developed in countries that are more integrated in the global economy, experience higher levels of liberalisation, and receive more investment from foreign institutional investors." The core message of these two statements, both substantiated by empirical evidence, highlights exactly why this research aimed to alter the NIS theory in its classic form. Yet despite certain shortcomings, NIS

remains one of the most robust, dynamically-structured models for explaining a country's innovation output, especially considering the fact that most revolutionary innovations in the modern history have "relied largely on fluid communications among professionals and firms in each country" (LaPier 1998: 106).

Perhaps the greatest mental preoccupation for me in hindsight of the research has been the reflection on how the research could have been conducted differently, and if the alternative approaches would have produced more legitimate results in the end. Perhaps the biggest lesson learned throughout the journey was the fact that online data collection methods can be highly challenging in nature when implemented in social research. Access and validation both arose to be major obstacles in the way of analysing weblog content. Also, as it emerged during the latter stages of the data analysis phase, settling for a pre-approved interviewee population can sometimes produce inconsistent results, regardless of how carefully the participants may have been vetted in terms of qualifications and expertise, and of the design of the interview questions.

It can be argued that the snowballing strategy employed to recruit the interviewees might have resulted in homogeneity of the consultants in terms of political views, although there was no solid proof of this, as data analysis showed that the participants' views were extremely diverse on nearly all counts. In order to avoid disciplinary bias, the interviewees were chosen equally from three distinct groups of scholars, journalists and activists. Extensive background checks were also conducted to shortlist only those experts with no known history of extremist conduct or radicalism. For instance, many potential candidates from the preliminary list were excluded due to concrete, publicly documented evidence of unconstructive response to the 2009 post-election unrest such as inciting violence through encouraging backlash or calling for foreign military intervention. While this research does not claim methodological perfection, it can confirm that reasonable steps were taken in the sampling of the interviewees to avoid any potential distortion of the final results. If I were in hindsight to redesign this element of the methodology, I would have probably elected to identify and narrow down the informants through active screening, which would have enabled much higher degrees of ideological diversity, as well as helping to more robustly safeguard the integrity of the collected data.

Looking back critically, there are many places where I would have conducted this research differently. First and foremost, not only I would have minimised the project's reliance on second-hand data either directly or by proxy (i.e. interviewees quoting media accounts), I would have also reduced the number of claims I was so highly tempted to make, placing instead the main emphasis on the empirical and theoretical qualification of the core arguments of the thesis. Moreover, I would have abstained from depending as much on online data by identifying and tapping into alternative, less limiting offline data streams, as well as having been more rigorous in both sampling and data interpretation processes. As with the expert interviews, I would have gone the extra mile to design a more robustly justified sampling process, in hope of producing more concrete results. But most importantly, I would have crafted more rigorous criteria for data analysis, and one that would allow sharper degrees of data triangulation. This would have been undoubtedly a major advantage in my search for deeper answers. With regards to the employed case studies, I would have dedicated a much larger ratio of my resources to study the Chinese NIS, which emerged in retrospect to hold more invaluable lessons compared to Ukraine for this research than I had previously anticipated.

Finally, the post-project reflections indicate to me that a scholarly researcher's personal beliefs and commitments can indeed influence the trajectory of an even well-designed research. While my background as an ex-local, Farsi speaking journalist and activist was crucial to my ability to undertake this PhD, my personal sentiments and aspirations proved at times to impose a limitation on, rather than providing a boost to, the authenticity of the results. In hindsight, I find each and every dilemma faced during the journey to have been an invaluable lesson in scholarly research, all of which have collectively helped me become better equipped for encountering any challenges that may arise in my future research endeavours.

Innovation Processes and Political Movements: Ideas for Future Research

This research suggests that a thorough, cross-border revision of NIS theory will not only extend its relevance to a greater part of the world, but will also help promote democracy around the world by addressing political barriers standing in the way of often highly talented cyber-activists' access to anti-censorship technologies. Further, it offers mechanisms for preventing regimes with poor track records on human rights from acquiring Western ICTs potentially useful in online censorship. This project was not able to establish a coherent relationship between CIS functionality and sociologically interrelated concepts such as political humour and viral qualities of modern communication. This was mainly due to a lack of time and funding, dictated by the conventional limitations of a full-time PhD programme.

Researchers interested in further exploring the field are best advised to stay sufficiently critical, if not sceptical, of static, deterministic approaches. They should design and prioritise their core aims and objectives in strict accordance with available resources. It will be vital that they understand the perils of pre-conceived theoretical and methodological biases for the validity and practicality of the outcomes of their research. Also, while funding, access and validation continue to be hurdles in the way of researching the emergence and use of online technologies in repressive countries, working closely with influential Western stakeholders such as the European Parliament could help overcome such problems.

Difficulty in gaining access to cyber-activists who often operate anonymously as well as an inability to penetrate into databases of governmental institutions both remained issues throughout this research. The latter is due to the secretive and intimidating nature of the Iranian regime, and the severe ethical complications that a hypothetical over-emphasis of the research design on retrieving guarded data could have imposed on this project. On the other hand, fluency in the Farsi language, as well as close familiarity with and direct knowledge of Iran's contextual realities proved to be invaluable to the successful completion of this thesis.

As the hard-line core of Iran's political elite is being pushed back by a moderate and reformist coalition for the first time since the end of President Khatami's government in 2005, it will become increasingly possible for Western legislators and academics to understand bottom-up socio-technical practices employed by Iranian pro-democracy cyber-activists. Policy solutions work best when government officials in both source and destination countries are open to at least some degree of positive interaction with one another. With anti-extremist currents presently and coincidentally in charge of both Iran and the United States, the circumstances seem even more suitable for the European Union to weigh in as a potent liberalist force in favour of democratisation. In this light, major future research opportunities for STS scholars interested in the subjects of this thesis to engage in more in-depth exploration of the issues at hand, including the relationship between gender inequality and

innovation in dictatorial countries as well as empirical analyses of the influences of exiled diaspora communities on their homelands' online pro-democracy discourse via systematic online innovations. Well-timed studies can make a tangible difference to victims of political oppression across the globe. Goal-oriented, constructive cooperation among Western academic institutions and research centres, regardless of their disciplinary differences is highly recommended in order to accelerate democratic change in emerging economies. By establishing and expanding a dynamic, responsive interface between academia in its expanded sense and counter-censorship activism in autocratic states, it may be possible to introduce a new, collaborative framework capable of further utilising ICTs for democratic ends, and of better serving egalitarian developments everywhere.

Reference List

- Abbasi, F. and Hajihoseini, H. (2004) Evaluating Iranian National Innovation System. *Research Institute for Technological Development Studies, Iranian Research Organisation for Science and Technology*. Available from: http://www.icmim.ir/Files/Article/2008-11-05_08.25.23_Evaluating%20Iranian%20National%20Innovation%20System.pdf [Accessed 25 August 2011]
- Adams, W.C. (2010) Conducting Semi-structured Interviews. *Handbook of Practical Program Evaluation*: p. 365
- Aday, S., Farrell, H., Lynch, M., Sides, J. and Freelon, D. (2012) New Media and Conflict After the Arab Spring. *United States Institute of Peace*. Washington DC, USA
- Adham, K.A., Sarkam, S.F., Ghanie, S.K.M., Kasimin, H., Muhamad, N.S.A. and Said, M.F. (2015) A Cybernetics Approach to Inclusive Growth Analysis: A Case of One District. *Systemic Practice and Action Research*: 1–18. Published 4 April 2015. New York, NY, USA: Springer Science
- Agarwal, N., Lim, M. and Wigand, R.T. (2011) Collective Action Theory Meets the Blogosphere: A New Methodology. *Networked Digital Technologies*: 224–39
- Ahmadi, R. (2009) Iran's Nonviolent Revolution. *Foundation for Social Studies and Analysis Paper 113*. Published 31 July 2009
- Akamai (2013) The State of the Internet: The Full Report. *Akamai Technologies*. Available from: http://www.akamai.com/dl/akamai/akamai_soti_q113.pdf [Accessed 19 September 2013]
- Aking, A.I., Encina, C., Restivo, M. and Schwartz, M. (2012) Old Wine in a New Cask: Protest Cycles in the Age of the New Social Media. *Whitehead Journal of Diplomacy and International Relations*. **13**: p. 89
- Alef (2012) Governmentalisation of A Civil Affair. Published 26 September 2012. Available from: <http://alef.ir/vdcezf8zzjh8pzi.b9bj.html?167111> [Accessed 10 September 2013]
- Alimardani, M. (2011) Iranian Women's Struggle for Empowerment in Contemporary Iran. *Journal of Near and Middle Eastern Studies*. Department of Near and Middle Eastern Civilisations, University of Toronto. Toronto, Canada
- Aljazeera (2009) Iran Internet Law Sparks Suspicion. Published 20 July 2009. Available from: <http://www.aljazeera.com/news/middleeast/2009/07/2009720132832678525.html> [Accessed 12 September 2013]
- Aljazeera (2012a) Is Iran's Halal Internet Possible? Published 2 October 2012. Available from: <http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html> [Accessed 17 December 2013]

Aljazeera (2012b) Iranians Abroad Question Impact of Elections. Published 1 March 2012. Available from: <http://www.aljazeera.com/indepth/features/2012/02/201222075034498638.html> [Accessed 19 September 2013]

Aljazeera (2013) Is Iran Going Offline? Published 23 May 2013. Available from: <http://stream.aljazeera.com/story/201305230047-0022773> [Accessed 16 September 2013]

All Voices (2010) A New Twist to an Ancient Battle. *All Voices, Inc.* Published 6 January 2010. Available from: <http://www.allvoices.com/contributed-news/4952346-a-new-twist-to-an-ancient-battle> [Accessed 17 December 2013]

Al-Monitor (2013) Conservative Iran MP: Reformists Win Only in Free Elections. Published 22 October 2013. Available from: <http://iranpulse.al-monitor.com/index.php/2013/10/3099/conservative-iran-mp-reformists-win-only-in-free-elections> [Accessed 2 November 2013]

Altenburg, T., Schmitz, H. and Stamm, A. (2008) Breakthrough? China's and India's Transition from Production to Innovation. *World Development*. **36**(2): 325–44

Amable, B., Barré, R. and Boyer, R. (1997) Diversity, Coherence and Transformations of Innovation Systems. In: R. Barré, M. Gibbons, J. Maddox, B. Martin and P. Papon (Eds.) *Science in Tomorrow's Europe*. Paris, France: Economica International

American Foreign Policy Council (2012) Defence Dossier. *Issue 4*. Published August 2012. Washington DC, USA

American Thinker (2013) Iranians in Sham Presidential Election. Published 10 September 2013. Available from: http://www.americanthinker.com/blog/2013/06/iranians_in_sham_presidential_election.html [Accessed 12 September 2013]

Amnesty International UK (2013) Iran: Seriously Ill Blogger Hossein Ronaghi-Maleki Must Be Released from Jail. Published 30 August 2013. Available from: http://www.amnesty.org.uk/news_details.asp?NewsID=20942 [Accessed 21 September 2013]

Anand, A.I. (2005) An Analysis of Enabling vs. Mandatory Corporate Governance Structures Post Sarbanes-Oxley. *Harvard Law School, Harvard University*. Drafted 20 December 2005. Available from: <http://www.law.harvard.edu/faculty/hjackson/pdfs/Enabling%20governanc.pdf> [Accessed 1 October 2013]

Archibugi, D. (2004) The Schizophrenia of American Democracy. *Peace Review*. Published June 2004. **16**(2): 181–84

Arendt, H. (1951) The Origins of Totalitarianism. *Schocken Books*. New York City, NY, USA

Arendt, H. (1961) Between Past and Future: Eight Exercises in Political Thought. *Penguin Books*. New York City, NY, USA

Arnaudo, D., Alva, A., Wood, P. and Whittington, J. (2013) Political and Economic Implications of Authoritarian Control of the Internet. *Critical Infrastructure Protection*. 7: 3–19. Berlin/Heidelberg: Springer

Arocena, R., Göransson, B. and Sutz, J. (2014) Knowledge Policies and Universities in Developing Countries: Inclusive Development and the Developmental University. *Technology in Society*. Elsevier BV. Amsterdam, Netherlands

ARS Technica (2012) Iran Moving Ahead with Plans for National Intranet. *Condé Nast*. Published 10 April 2012. Available from: <http://arstechnica.com/tech-policy/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative> [Accessed 17 December 2013]

Asghari, H. (2010) Botnet Mitigation and the Role of ISPs: A Quantitative Study into the Role and Incentives of Internet Service Providers in Combating Botnet Propagation and Activity. *Delft University of Technology*. Delft, Netherlands. Available from: http://repository.tudelft.nl/assets/uuid:db5eac04-61f9-4e1d-8f6e-5cdf3613bf42/Hadis_Thesis_Final.pdf [Accessed 20 April 2011]

Asheim, B. and Gertler, M. (2005) The Geography of Innovation. In: J. Fagerberg, D.C. Mowery and R.R. Nelson (Eds.) *The Oxford Handbook of Innovation*: 291–317. Oxford University Press. Oxford, UK

Ashuri, T. (2013) Envisioning the Internet: Implementing Disruptive Innovation in Media Organisations. *First Monday*: 18(5)

ASL19 (2013) Warning about the Fake Version of Psiphon 3.0 for Windows. Published 27 Jun 2013. Available from: <https://asl19.org/۳-برای-وی-سایفون-جعلی-نسخه-مورد-هشدار> [Accessed 22 September 2013]

Assmann, D. and Stiller, J. (2014) Knowledge Spill-Overs in Cities: The Role of Imitation and Innovation. *ERSA Conference Papers (ersa14p1101)*. 54th ERSA Congress, November 2014. European Regional Science Association. St. Petersburg, Russia

Atkinson, R. and Flint, J. (2001) Accessing Hidden and Hard-to-reach Populations: Snowball Research Strategies. *Social Research Update*. 33(1): 1–4

Atlantic Council (2013) Iran: How a Third Tier Cyber Power Can Still Threaten the United States. Published 29 July 2013. Available from: <http://www.atlanticcouncil.org/publications/issue-briefs/iran-how-a-third-tier-cyber-power-can-still-threaten-the-united-states> [Accessed 18 December 2013]

Atlantic Wire (2011) The Web Collectively Protests Congress's Censorship Law. *The Atlantic Monthly Group*. Published 16 November 2011. Available from: <http://www.theatlanticwire.com/technology/2011/11/web-collectively-protests-congress-censorship-law/45068> [Accessed 17 September 2013]

Baker, L. (2010) The Unintended Consequences of US Export Restrictions on Software and Online Services for American Foreign Policy and Human Rights. *Harvard Journal of Law and Technology*. 23(2): 537–63

Balasubramanian, A., Kumar, A.H. and Venkatesan, R.P. (2014) An Optimized and Secured VPN with Web Service. *Networking and Communication Engineering*: **6**(2)

Barney, J.B. (1991) Firm Resources and Advantage. *Journal of Management*. **17**: 99–120

Baron, L.F. (2012) More than a Facebook Revolution: Social Movements and Social Media in the Egyptian Arab Spring. *International Review of Information Ethics*. Volume 18

Barreras, R. (2004) New York City's Needle Exchange Policy and the Intersection of Science, Activism and Politics: A Case Study of Activist Research and Social Change. *Unpublished Doctoral Dissertation*. The Graduate Centre, City University of New York. NY, USA

Barriball, L.K., and While, A. (1994) Collecting Data Using a Semi-Structured Interview: A Discussion Paper. *Journal of Advanced Nursing*. **19**(2): 328–35

Basden, A., Brooke, C., Russell, R. and Holt, P. (2011) In: J. Stoep and S. Strijbos (Eds.) *Religious Roots of Information Technology: From Technology Transfer to Intercultural Development*. p. 109

Bauer, M.W. (2009) The Evolution of Public Understanding of Science: Discourse and Comparative Evidence. *Science, Technology and Society*: **14**(2): 221–40

BBC (2002) Web Gives A Voice to Iranian Women. *British Broadcasting Corporation*. Published 17 June 2002. Available from: <http://news.bbc.co.uk/1/hi/sci/tech/2044802.stm> [Accessed 11 September 2013]

BBC (2007) Huge Cost of Iranian Brain Drain. *British Broadcasting Corporation*. Published 08 Jan 2007. Available from: http://news.bbc.co.uk/1/hi/world/middle_east/6240287.stm [Accessed 04 December 2013]

BBC (2009a) Hi-tech Helps Iranian Monitoring. *British Broadcasting Corporation*. Published 22 June 2009. Available from: <http://news.bbc.co.uk/1/hi/technology/8112550.stm> [Accessed 12 September 2013]

BBC (2009b) Internet Brings Events in Iran to Life. *British Broadcasting Corporation*. Published 15 June 2009. Available from: <http://news.bbc.co.uk/1/hi/8099579.stm> [Accessed 12 September 2013]

BBC (2010) MEPs Condemn Nokia Siemens Surveillance Tech in Iran. *British Broadcasting Corporation*. Published 11 February 2010. Available from: <http://news.bbc.co.uk/1/hi/8511035.stm> [Accessed 19 September 2013]

BBC (2012) Google Search and Gmail Censored in Iran. *British Broadcasting Corporation*. Published 24 September 2012. Available from: <http://www.bbc.co.uk/news/technology-19700910> [Accessed 16 September 2013]

BBC (2013) Iran Arrests 11 Journalists with Foreign Contacts. *British Broadcasting Corporation*. Published 28 January 2013. Available from: <http://www.bbc.co.uk/news/world-middle-east-21230687> [Accessed 10 December 2013]

BBC Persian (2011) Ministry of Science, Research and Technology: 250,000 Highly Skilled Iranian Migrants Reside in North America. *British Broadcasting Corporation*. Published 14 February 2011. Available from: http://www.bbc.co.uk/persian/iran/2011/02/110214_128_250_thousand_iranian_specialists_america.shtml [Accessed 4 December 2013]

BBC Persian (2013) Will Iran's National Internet Mean No World Wide Web? *British Broadcasting Corporation*. Published 27 April 2013. Available from: <http://www.bbc.co.uk/news/world-middle-east-22281336> [Accessed 10 September 2013]

Bebbington, A. (2001) Indigenous Knowledge and Technology. *International Encyclopaedia of Social and Behavioural Sciences*: 7289–92. Elsevier Science Ltd. Oxford, UK

Beduya, M. (2009) Learning Interactions Make for National Innovation Systems. *SYNTHESiST*. Published 30 December 2009. Available from: <http://synthesistblog.com/learning-interactions-make-for-national-innovation-systems-154-0> [Accessed 12 October 2013]

Beeman, W.O. (2009) The Economics of the Downtrodden: Revolutionary Ideology and Practical Politics in the Islamic Republic of Iran. Paper prepared for USC College Conference. *Iranian Economy at a Crossroads: Domestic and Global Challenges*. 18–19 September 2009. Davidson Conference Centre, University of Southern California. CA, USA

Belward, A. (2013) Europe's Relations with the Wider World: A Unique View from Space. In: *European Identity through Space*: 119–31. Vienna, Austria: Springer

Bengry-Howell, A., Wiles, R., Nind, M. and Crow, G. (2011) A Review of the Academic Impact of Three Methodological Innovations: Netnography, Child-Led Research and Creative Research Methods. *ESRC National Centre for Research Methods Working Paper Series 01/11*. NCRM Hub, University of Southampton. Southampton: UK

Bierema, L. (2003) The Role of Gender Consciousness in Challenging Patriarchy. *International Journal of Lifelong Education*. **22**(1): 3–12

Biernacki, P. and Waldorf, D. (1981) Snowball Sampling: Problems and Techniques of Chain Referral Sampling. *Sociological Methods and Research*. **10**(2): 141–63

Bijker, W.E., Hughes, T.P. and Pinch, T. (1987) The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. Cambridge, MA, USA: MIT Press

Blanke, J. (2005) Assessing Ukraine's Competitiveness Amid Political Change. *Centre for Strategic Insight, World Economic Forum*. Available from: <http://www.weforum.org/pdf/ukrainecompetitiveness.pdf> [Accessed 15 October 2013]

Bloomberg (2011) Iranian Police Seizing Dissidents Get Aid Of Western Companies. *Bloomberg L.P.* Published 31 October 2011. Available from: <http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html> [Accessed 12 September 2013]

- Borrus, M. (1997) Left for Dead: Asian Production Networks and the Revival of US Electronics. Published April 1997. *Berkeley Roundtable on the International Economy (BRIE) Working Paper 100*. USA: University of California, Berkeley
- Borup, M., Brown, N., Konrad, K. and Van Lente, H. (2006) The Sociology of Expectations in Science and Technology. *Technology Analysis and Strategic Management*. **18**(3–4): 285–98
- Boudreau, K.J. and Lakhani, K.R. (2013) Using the Crowd as an Innovation Partner. *Harvard Business Review*. Published April 2013. Available from: <http://hbr.org/2013/04/using-the-crowd-as-an-innovation-partner> [Accessed 1 October 2013]
- Bowman, W.M. and Camp, L.J. (2013) Protecting the Internet from Dictators: Technical and Policy Solutions to Ensure Online Freedoms. *The Innovation Journal*
- Bozzoli, C. and Brück, T. (2011) Revolutionaries and Counterrevolutionaries: Longitudinal Evidence from Ukraine's Orange Revolution. *German Institute for Economic Research*. Paper Presented on Saturday 27 August 2011 at the European Economic Association and Econometric Society Parallel Meetings, 25–29 August 2011. Oslo, Norway
- Branstetter, L.G. (2001) Are Knowledge Spill-Overs International or Intra-National in Scope? Micro-Econometric Evidence from the US and Japan. *Journal of International Economics*. **53**(1): 53–79
- Bresheeth, H. (2012) The Arab Spring: A View from Israel. *Middle East Journal of Culture and Communication*. **5**(1): 42–57
- Breuer, F. and Roth, W.M. (2003) Subjectivity and Reflexivity in the Social Sciences: Epistemic Windows and Methodical Consequences. Published May 2003. In: *Forum Qualitative Social Research* **4**(2)
- Brookings Institution (2013) State of Play as Iran's Epic Campaign Grinds to an End. Published 13 June 2013. Available from: <http://www.brookings.edu/blogs/iran-at-saban/posts/2013/06/12-campaign-end> [Accessed 1 October 2013]
- Brooklyn Institute for Social Research (2012) The Simmering Period: Iran, After 2009. Published March 2012. Available from: <http://thebrooklyninstitute.com/2012/03/02/the-simmering-period-iran-after-2009-a-supplemental-podcast-for-social-research> [Accessed 5 December 2013]
- Bryman, A. (2012) Social Research Methods. Oxford, UK: *Oxford University Press*
- Bugliarello, G. (2011) Engineering and Sustainable Development: Fostering Technology, Innovation and Production. *International Science, Technology and Innovation Centre for South-South Cooperation, UNESCO*. **41**
- Burenstam-Linder, S. (1961) An Essay on Trade and Transformation. *Doctoral Dissertation*. University of Gävle. Gävle, Sweden

- Burgett, B., Kochhar-Lindgren, K., Krabill, R. and Thomas, E. (2013) The Affirmative Character of Cultural Studies. *International Journal of Cultural Studies*. **16**(4): 419–39
- Burns, A. and Eltham, B. (2009) Twitter Free Iran: An Evaluation of Twitter's Role in Public Diplomacy and Information Operations in Iran's 2009 Election Crisis. *Record of the Communications Policy and Research Forum 2009*. Pages: 298–310
- Business Year (2011) Iran: Access and Quality. Available from: <http://www.thebusinessyear.com/publication/article/7/637/iran-2011/access-and-quality> [Accessed 5 October 2013]
- Callahan, K. (2006) Elements of Effective Governance: Measurement, Accountability and Participation. Boca Raton, Florida, USA: *CRC Press*
- Cappelli, R., Czarnitzki, D. and Kraft, K. (2014) Sources of Spill-Overs for Imitation and Innovation. *Research Policy*. **43**(1): 115–120
- Carlsson, B. and Stankiewicz, R. (1991) On the Nature, Function and Composition of Technological Systems. *Journal of evolutionary Economics*: **1**(2): 93–118
- Carlsson, B. (2006) Internationalisation of Innovation Systems: A Survey of the Literature. *Research Policy*. **35**(1): 56–67
- Carpenter, R.G. (2009) Political Spaces and Remediated Places: Rearticulating the Role of Technology in the Writing Centre. *Doctoral Dissertation*. University of Central Florida. Orlando, Florida, USA
- Casas, M. (2006) Wan and Activist Research: Toward Building De-Colonial and Feminist Projects. *World Anthropologies Network*: p. 75
- Castells, M. (1996) The Rise of the Network Society. *The Information Age: Economy, Society and Culture*. **1**(1996): 1–25. Oxford, UK: *Blackwell Publishers*
- CBS Interactive (2010) Nokia-Siemens Networks Respond to Iran Human Rights Abuses Claims. *ZDNet*. Published 20 August 2010. Available from: <http://www.zdnet.com/blog/sustainability/nokia-siemens-networks-respond-to-iran-human-rights-abuses-claims/1351> [Accessed 1 October 2013]
- CBS Interactive (2012) Iran's Deadly Cyber Police: Indefinite Detention and Execution for Netizens. *ZDNet*. Published 16 February 2012. Available from: <http://www.zdnet.com/blog/violetblue/irans-deadly-cyber-police-indefinite-detention-and-execution-for-netizens/981> [Accessed 10 December 2013]
- Centre for a Democratic Iran (2012) How to Bypass Internet Filtering in Iran. Published 15 November 2012. Available from: http://www.cdi-iran.org/Article/1280-How_to_bypass_Internet_Filtering_in_Iran [Accessed 17 September 2013]
- Chaminade, C. and Vang, J. (2008) Globalisation of Knowledge Production and Regional Innovation Policy: Supporting Specialised Hubs in the Bangalore Software Industry. *Research Policy*. **37**(10): 1684–96

- Chang, P.L. and Shih, H.Y. (2005) Comparing Patterns of Inter-Sectoral Innovation Diffusion in Taiwan and China: A Network Analysis. *Technovation*. **25**(2): 155–69
- Chardy, M., Ouorou, A. and Van Donselaar, T. (2012) Optimisation of Internet Interconnection Policy in the Top Per centile Pricing Framework. *Optimisation and Engineering*. **13**(1): 151–68
- Charles, M. (2011) What Gender Is Science? *Contexts*. **10**(2): 22–8. American Sociological Association. Washington DC, USA
- Chen, D. (2004) Gender Equality and Economic Development: The Role for Information and Communication Technologies. *World Bank Policy Research Working Paper* 3285
- Chen, S.H. (2004) Taiwanese IT Firms' Offshore R&D in China and the Connection with the Global Innovation Network. *Research Policy*. **33**(2): 337–49
- Chen, Y. and Xiao, F. (2011) Review of the Techno-Feminism. *Science, Technology and Dialectics*. **1**: 67–72
- Cheng, G., Cohen, M., Green, J., Oliviera, C. and Stadnyk, M. (2011) Responses to Questions Posed by CNAS on International Law and Internet Freedom. *The Harvard Law National Security Research Group*. Available from: <http://www.law.harvard.edu/students/orgs/nsrc/CNAS-Final%20Draft-3.pdf> [Accessed 20 April 2011]
- Chokoshvili, D. (2011) The Role of the Internet in Democratic Transition: Case Study of the Arab Spring. *Central European University*. Budapest, Hungary
- Choudry, A. (2013) Activist Research Practice: Exploring Research and Knowledge Production for Social Action. *Socialist Studies*: **9**(1)
- Christoffersen, L., Modéer, K.Å. and Andersen, S. (2010) Law and Religion in the 21st Century: Nordic Perspectives. Copenhagen, Denmark: *Djøf Publishing*
- Cimoli, M. and Porcile, G. (2010) Specialisation, Wage Bargaining and Technology in a Multi-Goods Growth Model. *Metroeconomica*. **61**(1): 219–238
- Citizen Lab (2012) Iranian Anti-censorship Software Simurgh Circulated with Malicious Backdoor. *University of Toronto*. Toronto, Canada. Published 25 May 2012. Available from: <https://citizenlab.org/wp-content/uploads/2012/08/04-2012-iranianticensorship.pdf> [Accessed 19 September 2013]
- Clark, A. (2011) The Relevance of Nonviolent Struggle to Domestic Change in Iran. *Journal of International Service*. Published Fall 2011. Available from: <https://www.american.edu/sis/jis/upload/2ClarkF11.pdf> [Accessed 19 September 2013]
- Code, L. (2012) Taking Subjectivity into Account. Netherlands: *Springer*. pp. 85–100
- Collins, H.M. and Evans, R. (2002) The Third Wave of Science Studies, Studies of Expertise and Experience. *Social Studies of Science*. **32**(2): 235–96

Cordesman, A.H. (2007) Iran's Revolutionary Guards, the Al-Quds Force and Other Intelligence and Paramilitary Forces. Published 16 August 2007. *Centre for Strategic and International Studies (CSIS)*. Washington DC, USA

Cordesman, A.H. and Seitz, A.C. (2009) Iranian Weapons of Mass Destruction: The Birth of a Regional Nuclear Arms Race? *Centre for Strategic and International Studies*. Washington DC, USA

CNN (2010) Iran Arrests 30 Accused of US-Backed Cyber War. *Cable News Network*. Published 14 Mar 2010. Available from: <http://edition.cnn.com/2010/WORLD/meast/03/13/iran.cyber.arrests/index.html> [Accessed 19 September 2013]

CNN (2013) Forbidden Voices: Female Bloggers Fight for Freedom of Speech. *Cable News Network*. Published 03 May 2013. Available from: <http://edition.cnn.com/2013/05/03/world/world-press-freedom-day-forbidden-voices> [Accessed 11 September 2013]

Cooke, P. (1992) Regional Innovation Systems: Competitive Regulation in the New Europe. *Geoforum*. **23**(3): 365–82

Dabashi, H. (2011) The Green Movement in Iran. Piscataway, New Jersey, USA: *Transaction Publishers*

Dahl, R.A. (2000) On Democracy. Connecticut, USA: *Yale University Press*

Dahlberg, A. (2014) Arbitration in China: A Legal and Cultural Analysis by Kun Fan (Book Review). *Transnational Dispute Management*. **11**(3)

Daily Aztec (2011) Facebook Provides Outlet for Dissent. Published 22 February 2011. Available from: <http://www.thedailyaztec.com/2011/02/facebook-provides-outlet-for-dissent> [Accessed 10 December 2013]

Daily Mail (2013) Tony Blair: Europe Must Change, But Most Britons Want to Stay in and Now I Want to Mobilise Them. *Associated Newspapers Ltd*. Published 26 January 2013. Available from: <http://www.dailymail.co.uk/news/article-2268918/Tony-Blair-warns-leaving-European-Union.html> [Accessed 8 October 2013]

Daily Reveille (2013) University Sees Influx of Iranian Students. Published 8 April 2013. Available from: http://www.lsurreveille.com/news/article_0a4aefc8-a0a0-11e2-b096-001a4bcf6878.html [Accessed 4 December 2013]

Dale, H.C. and Phillips, J. (2010) Support for Iran's Green Revolution Gains Traction in the Senate. *The Heritage Foundation*. Paper Number 2806. Published 17 February 2010. Washington DC, USA

Dana Khabar (2013) Don't Be Too Surprised If VPNs Are Disabled for Good. Published 11 Mar 2013. Available from: <http://danakhabar.com/fa/news/1153152/> - اگر برای همیشه وی پی ان ها از کار افتاد تعجب نکنید [Accessed 10 September 2013]

- Danielyan, H. and Wittbom, E. (2009) National Innovation Systems in Two Nordic Countries: Sweden and Finland. *Thesis for the Master's Degree in Business Administration (MBA)*. Published Autumn 2009. School of Management, Blekinge Institute of Technology. Valhallavägen, Stockholm, Sweden
- Danilda, I. and Granat Thorslund, J. (2011) *Innovation and Gender*. Stockholm, Sweden: Vinnova
- Dawoody, A.R. (2011) The Global Participant-Observer: Emergence, Challenges and Opportunities. *The Innovation Journal*. **16**(1): Article 9
- Dawoody, A.R. (2015) *Public Administration and Policy in the Middle East*. New York, NY, USA: Springer International Publishing AG
- Deibert, R.J. (2008) The Geopolitics of Internet Control: Censorship, Sovereignty and Cyberspace. In: A. Chadwick and P.N. Howard (Eds.) *Routledge Handbook of Internet Politics*. pp. 323–36. New York, NY, USA: Routledge
- Deibert, R.J. and Rohozinski, R. (2007) Good for Liberty, Bad for Security? Global Civil Society and the Securitisation of the Internet. *Massachusetts Institute of Technology*. Cambridge, MA, USA. Available from: <http://www.wsir.pwias.ubc.ca/2007/articles/DeibertRohozinskiDraftChapter-Access%20Denied%20-%20MIT.pdf> [Accessed 20 April 2011]
- Deibert, R.J. and Rohozinski, R. (2010) Cyber Wars. *Index on Censorship*. Available from: <http://www.eurozine.com/pdf/2010-03-26-deibert-en.pdf> [Accessed 20 April 2011]
- Deng, P. (2007) Investing for Strategic Resources and Its Rationale: The Case of Outward FDI from Chinese Companies. *Business Horizons*. **50**(1): 71–81
- Denning, D.E. (2007) Assessing the Computer Network Operations Threat of Foreign Countries. Available from: <http://www.dtic.mil/dtic/tr/fulltext/u2/a484697.pdf> [Accessed 20 April 2011]
- Denzin, N.K. (2009) The Elephant in the Living Room: Extending the Conversation about the Politics of Evidence. *Qualitative Research*. **9**(2): 139–60
- Deutsche Welle (2012) EU and China: A Troubled Relationship. Published 19 Nov 2012. Available from: <http://www.dw.de/eu-and-china-a-troubled-relationship/a-16385898> [Accessed 7 October 2013]
- Deutsche Welle (2013) Psiphon Helps Dodge the Online Trackers. Published 23 April 2013. Available from: <http://www.dw.de/psiphon-helps-dodge-the-online-trackers/a-16765092> [Accessed 17 September 2013]
- De Ville, F. and Orbie, J. (2013) The European Commission's Neoliberal Trade Discourse Since the Crisis: Legitimising Continuity Through Subtle Discursive Change. *The British Journal of Politics and International Relations*. **16**(1): 149–67

- Dewey, T., Kaden, J., Marks, M., Matsushima, S. and Zhu, B. (2012) The Impact of Social Media on Social Unrest in the Arab Spring. *Final Report Prepared for Defence Intelligence Agency*. International Policy Program, Stanford University. Stanford, CA, USA
- Doloreux, D. (2002) What We Should Know about Regional Systems of Innovation. *Technology in Society*. **24**(3): 243–63
- Donya-E-Eqtesad (2013a) "We Will Be Selling VPNs, But They Are Not to Be Used for Anti-filtering Purposes." Published 03 July 2013. Available from: <http://www.donya-e-eqtesad.com/news/736316> [Accessed 10 September 2013]
- Donya-E-Eqtesad (2013b) Failure of the Domestic VPN Project. Published 21 August 2013. Available from: <http://www.donya-e-eqtesad.com/news/734451> [Accessed 10 September 2013]
- Drezner, D.W. (2010) Weighing the Scales: The Internet's Effect on State-Society Relations. *Brown Journal of World Affairs*. **16**(2): 31–44
- Dubowitz, M. (2013) Iran's Islamic Revolutionary Guard Corps: Guardians of the Revolution and Violators of Human Rights. *Foundation for Defence of Democracies*. Testimony before the International Human Rights Subcommittee, House of Commons, Parliament of Canada. 30 May 2013. Ottawa, ON, Canada
- Duda, A. (2010) When It's Time to Say Enough! Youth Activism before and during the Rose and Orange Revolutions in Georgia and Ukraine. *Centre for Russian and East European Studies, University of Birmingham*. Birmingham, UK. Available from: <http://etheses.bham.ac.uk/1108/1/Duda10PhD.pdf> [Accessed 8 August 2012]
- Duffy, M.J. (2010) Code Orange: How the Internet, Cell Phones and New Technologies Helped Shape the Ukrainian Revolution of 2004. *The Atlanta Review of Journalism History*. Published Fall 2010. **9**: 73–88
- Dutton, W.H. (1996) Information and Communication Technologies: Visions and Realities. Oxford, UK: *Oxford University Press*
- Dyczok, M. (2004) The Politics of Media in Ukraine: Election 2002. *Paper submitted after the workshop 'Media and Politics in Ukraine' presented by the Petro Jacyk Programme for the study of Ukraine at the University of Toronto on 19 April 2004*. Toronto, Canada
- Dyczok, M. (2005) Breaking Through the Information Blockade: Election and Revolution in Ukraine 2004. *Canadian Slavonic Papers*. **47**(3–4): 241–64. September–December 2005
- Dyczok, M. (2006) Was Kuchma's Censorship Effective? Mass Media in Ukraine before 2004. *Europe-Asia Studies*. March 2006. **58**(2): 215–38
- Eagly, A.H. and Steffen, V.J. (1986) Gender and Aggressive Behaviour: A Meta-Analytic Review of the Social Psychological Literature. *Psychological Bulletin*. **100**(3): 309–30. American Psychological Association, Inc. Washington DC, USA

Earl, J., and Kimport, K. (2011) Digitally Enabled Social Change: Activism in the Internet Age. Cambridge, MA, USA: *MIT Press*

Economist (2010) Democracy Index 2010: Democracy in Retreat. Available from: http://graphics.eiu.com/PDF/Democracy_Index_2010_web.pdf [Accessed 12 July 2011]

Eddy, M. (2013) PirateBrowser Beats Blockades, Doesn't Make You Invisible to NSA. *Ziff Davis, LLC*. Published 12 August 2013. NY, USA. Available from: <http://uk.pcmag.com/opinion/13639/piratebrowser-beats-blockades,-doesnt-make-you-inv> [Accessed 03 September 2014]

Edwards, B., Revill, J. and Bezuidenhout, L. (2014) From Cases to Capacity? A Critical Reflection on the Role of Ethical Dilemmas in the Development of Dual-Use Governance. *Science and Engineering Ethics*. **20**(2): 571–82

Ekwo, U. (2012) Media-Politics Complex in the Era of Media Convergence: Lessons from the Arab Spring. *Centre for Media and Peace Initiatives*. NY, USA

Elleman, M. (2013) Gulf I: Iran's Power in the Air. *United States Institute of Peace*. Published 11 March 2013. Available from: <http://iranprimer.usip.org/blog/2013/mar/11/gulf-i-iran-s-power-air> [Accessed 18 December 2013]

Ellinas, C., Hall, M.J. and Hultin, A. (2014) Design Through Failure: A Network Perspective. In *Proceedings of 'Design 2014', 13th International Design Conference*. 19–22 May 2014. Cavtat, Dubrovnik, Croatia

Ergul, F.A. (2012) Communicative Turn of IR in Analysing the Arab Spring. *Paper Presented on 10 July 2012 at the 22nd World Congress of Political Science*. Madrid, Spain

Ernst, D. (2002) Global Production Networks and the Changing Geography of Innovation Systems: Implications for Developing Countries. *Economics of Innovation and New Technology*. **11**(6): 497–523

Ernst, D. (2006) Innovation Off-Shoring: Asia's Emerging Role in Global Innovation Networks. *East-West Centre Special Report 10*. Honolulu, Hawaii, USA

Ernst, D. and Guerrieri, P. (1998) International Production Networks and Changing Trade Patterns in East Asia: The Case of the Electronics Industry. *Oxford Development Studies*. **26**(2): 191–212

Ervasti, H., Fridberg, T., Hjerm, M. and Ringdal, K. (2008) Nordic Social Attitudes in a European Perspective. Cheltenham, UK: *Edward Elgar Publishing Ltd*.

Estacio, E.V. (2012) Playing with Fire and Getting Burned: The Case of the Naïve Action Researcher. *Journal of Community and Applied Social Psychology*. **22**(5): 439–51

Etzkowitz, H. and Leydesdorff, L. (2000) The Dynamics of Innovation: From National Systems and Mode 2 to a Triple Helix of University-Industry-Government Relations. *Research policy*. **29**(2): 109–23

Etzkowitz, H., Dzisah, J., Ranga, M. and Zhou, C. (2007) The Triple Helix Model for Innovation: The University-Industry-Government Interaction. *Asia Pacific Tech Monitor*. **24**(1): 14–23

European Commission (2009) Setting Up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items. *Official Journal of the European Union*. Available from: http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf [Accessed 18 July 2011]

European Parliament (2010) Situation in Iran: European Parliament Resolution of 10 February 2010 on Iran. Available from: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2010-0016+0+DOC+WORD+V0//EN> [Accessed 20 April 2011]

European Voice (2010) Outwitting Iran's Cyber Censors. Available from: <http://www.europeanvoice.com/article/imported/outwitting-iran-s-cyber-censors-/67951.aspx> [Accessed 11 September 2013]

Eyben, R. (2015) Uncovering the Politics of Evidence and Results. In: I. Guijt and R. Eyben (Eds.) *The Politics of Evidence and Results in International Development: Playing the Game to Change the Rules*. pp. 19–38. Rugby, Warwickshire, UK: Practical Action Publishing Ltd.

Eysenbach G. and Till, J.E. (2001) Ethical Issues in Qualitative Research on Internet Communities. *BMJ*. Published 10 November 2001. **323**: 1103–5

Fagerberg, J., Mowery, D.C. and Verspagen, B. (2009) The Evolution of Norway's National Innovation System. *Science and Public Policy*. **36**(6): 431–44

Fan, P. (2006) Catching Up through Developing Innovation Capability: Evidence from China's Telecom and Equipment Industry. *Technovation*. **26**(3): 359–68

Farhi, F. (2008) Iran's 2008 Majlis Elections: The Game of Elite Competition. *Middle East Brief No. 29*. Crown Centre for Middle East Studies, Brandeis University. Waltham, Massachusetts, USA. Published 9 May 2008. Available from: <http://www.brandeis.edu/crown/publications/meb/MEB29.pdf> [Accessed 02 November 2013]

Farivar, C. (2011) *The Internet of Elsewhere: The Emergent Effects of a Wired World*. NJ, USA: Rutgers University Press

Faulkner, W. (2001) The Technology Question in Feminism: A View from Feminist Technology Studies. *Women's Studies International Forum*. Published February 2001. **24**(1): 79–95. Oxford, UK: Pergamon Press

Feenberg, A. (2006) A Democratic Internet? *Paper Delivered on 17 November 2006 at the Freedom of Expression Foundation*. Oslo, Norway. Available from: <http://www.sfu.ca/~andrewf/demint.htm> [Accessed 2 November 2013]

Feijt, L. (2012) Europe in Conflict! An analysis on the Position of the EU When Mediating Between Neighboring Countries. *Paper for the 2012 Edition of the International [Post]graduate Course on Inclusion and Exclusion in Contemporary European Societies, 'Challenges of Europe: The Strength of Soft Power.'* 16–20 April 2012. Dubrovnik, Croatia. Available from: http://www.inclusionexclusion.eu/site/wp-content/uploads/2012/07/FeijtLuuk_2012.06.01_paper.pdf [Accessed 8 October 2013]

Fielding, N.G. (2012) Triangulation and Mixed Methods Designs Data Integration with New Research Technologies. *Journal of Mixed Methods Research*. **6**(2): 124–36

Figliola, P.M., Nakamura, K.H., Addis, C.L. and Lum, T. (2010) US Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology. *Congressional Research Service*. Available from: <http://www.fas.org/sgp/crs/misc/R41120.pdf> [Accessed 20 April 2011]

Filippova, O. (2005) Anti-Orange Discourses in Ukraine: A Cyber Ethnography of the Political Opposition. *Paper Presented at the First Annual Danyliw Seminar in Contemporary Ukrainian Studies*. 29 September–1 October 2005. University of Ottawa. Ottawa, ON, Canada

Financial Times (2008) Iranians Defy Censor with Bootleg DVDs. *Financial Times*. Published 5 April 2008. Available from: <http://www.ft.com/cms/s/0/709a7ee4-029c-11dd-9388-000077b07658.html#axzz2ebj0IRpb> [Accessed 11 September 2013]

Financial Times (2011) Airy Talk of 'Good' And 'Bad' Business Is Wide of the Mark. *Financial Times*. Published 30 Sep 2011. Available from: <http://www.ft.com/cms/s/0/4d1ec854-ea96-11e0-b0f5-00144feab49a.html#axzz2mY0j1yAU> [Accessed 3 December 2013]

Fine, M. (2006) Bearing Witness: Methods for Researching Oppression and Resistance: A Textbook for Critical Research. *Social Justice Research*. **19**(1): 83–108

Finlay, L. and Gough, B. (2003) Reflexivity: A practical Guide for Researchers in Health and Social Sciences. Blackwell Science, Ltd. Oxford, UK

Flanagin, A.J., Flanagin, C. and Flanagin, J. (2010) Technical Code and the Social Construction of the Internet. *New Media and Society*. **12**(2): 179–96

Floss Manuals (2011) How to Bypass Internet Censorship: Using Sabz Proxy. Berlin, Germany. Available from: http://en.flossmanuals.net/bypassing-censorship/ch014_using-sabzproxy [Accessed 17 September 2013]

Forbes (2013) An Injection of Rule of Law for Ukrainian Business? Oligarch's Lawsuit Could Help Improve the Culture of Business Dealings in the Post Soviet Space. *Forbes.com LLC*. Published 15 July 2013. Available from: <http://www.forbes.com/sites/melikkaylan/2013/07/15/an-injection-of-rule-of-law-for-ukrainian-business-oligarchs-lawsuit-could-help-improve-the-culture-of-business-dealings-in-the-post-soviet-space> [Accessed 15 October 2013]

- Forster, L. (2006) Importing Orange? Prospects for Belarusian Democratisation. Hamilton College. NY, USA. Available from: <http://www.hamilton.edu/documents/levitt-center/Importing%20orange.pdf> [Accessed 8 August 2012]
- Franzese, R.J. (2014) Three Essays on the Political Economy of International Taxation and Investment. *Doctoral Dissertation*. University of Michigan. Detroit, Michigan, USA
- Freedom House (2011) Country Report for End Users in Iran. Washington DC, USA. Available from: http://freedomhouse.org/images/File/special_reports/LOtF_Iran.pdf [Accessed 28 July 2011]
- Freedom House (2012) Freedom on the Net: A Global Assessment of Internet and Digital Media. Washington DC, USA. Available from: <http://www.freedomhouse.org/sites/default/files/FOTN%202012%20summary%20of%20findings.pdf> [Accessed 31 August 2013]
- Freedom House (2013a) Freedom on the Net: 2013 Global Scores. Washington DC, USA. Available from: http://www.freedomhouse.org/sites/default/files/resources/FOTN%202013_Charts%20and%20Graphs_Global%20Scores.pdf [Accessed 4 October 2013]
- Freedom House (2013b) Freedom on the Net: Iran. Washington DC, USA. Available from: http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Iran.pdf [Accessed 4 October 2013]
- Freeman, C. (1982) Technological infrastructure and international competitiveness, *Draft Paper Submitted to the OECD Ad Hoc Group on Science, Technology and Competitiveness*. Paris, France: OCDE
- Freeman, C. (1987) Technology Policy and Economic Performance: Lessons from Japan. London, United Kingdom: Frances Pinter
- Freeman, C. (1995) The National System of Innovation in Historical Perspective. *Cambridge Journal Of Economics*. **19**(1): 5–24
- Freeman, C. (2002) Continental, National and Sub-National Innovation Systems: Complementarity and Economic Growth. *Research Policy*. **31**(2): 191–211
- Frickel, S., Gibbon, S., Howard, J., Ottinger, G. and Hess, D. (2009) Undone Science: Charting Social Movement and Civil Society Challenges to Research Agenda Setting. *Science, Technology and Human Values*
- Fritsch, S. (2011) Technology and Global Affairs. *International Studies Perspectives*. **12**(1): 27–45
- Fu, X. and Gong, Y. (2008) Direct Technical Change, Indigenous and Foreign Innovation Efforts and Drivers of Technology Upgrading: Evidence from China. *Conference Confronting the Challenge of Technology for Development: Experiences from the BRICS*. Sanjaya Lall Program for Technology and Management. QEH, University of Oxford. Oxford, UK

- Fu, X., Li, Y. and Si, Y. (2013) The impact of Paternalistic Leadership on Innovation: An Integrated Model. *Nankai Business Review International*. **4**(1): 9–24
- Fukuyama, F. (1996) Trust: The Social Virtues and the Creation of Prosperity. Volume 457. New York, NY, USA: Free Press
- Fuller, G. (1995) The Next Ideology. *Foreign Policy*. **98**: 145–58
- Gadzetomania (2009) Hakerzy Walą w Iran z "Działą Jonowego". *Gadzetomania.pl*. Published 15 June 2009. Available from: <http://internet.gadzetomania.pl/2009/06/15/hakerzy-wala-w-iran-z-dziala-jonowego> [Accessed 22 September 2013]
- Galland, A., Abiteboul, S., Marian, A. and Senellart, P. (2010) Corroborating Information from Disagreeing Views. In: *Proceedings of the Third ACM International Conference on Web Search and Data Mining*. Published February 2010. pp. 131–40
- Gammelgård, M., Ekstedt, M. and Närman, P. (2007) Architecture Scenario Analysis: Estimating the Credibility of the Results. In: *Seventeenth Annual Symposium of the International Council on Systems Engineering*. Held 24–28 June 2007. San Diego, CA, USA
- Ganji, M., Dehghantanha, A., Izura-Udzir, N. and Damshenas, M. (2013) Cyber Warfare Trends and Future. *Advances in Information Sciences and Service Sciences*. **5**(13). Published August 2013. Busan, Korea
- Ganor, B. (1998) Countering State-Sponsored Terrorism. *International Institute for Counter-Terrorism*. Published 25 April 1998. Available from: <http://www.ict.org.il/Articles/tabid/66/Articlsid/701/currentpage/34/Default.aspx> [Accessed 12 October 2013]
- Gerdab (2010) If Using Proxy Software and VPNs is a Crime, What Is the Punishment? Published 30 December 2010. Available from: <http://www.gerdab.ir/fa/news/3596/-اگر-استفاده-vpn-از-فیلتر شکن-و-جرم-است-مجازات-آن-چیست> [Accessed 10 September 2013]
- Ghazinoori, S. (2004a) Extracting Strategies for Repairing National Innovation System of Iran Based on SWOT Analysis. *Bu-Ali Sina University*. Hamedan, Iran. Available from: <http://www.hitechpark.com/files/pdf/c.pdf> [Accessed 9 November 2011]
- Ghazinoori, S. (2004b) Technology Management System in Iran: Organisation, Programs, Challenges. *Bu-Ali Sina University*. Hamedan, Iran. Available from: <http://www.tco.ac.ir/research/10-Ghazinouri.pdf> [Accessed 10 September 2011]
- Gladwin, J., Dixon, R.A. and Wilson, T.D. (2003) Implementing a New Health Management Information System in Uganda. *Health Policy and Planning*. **18**(2): 214–24. Oxford, UK: Oxford University Press
- Global Information Society Watch (2011) The Internet and Civil Resistance: Freedoms and State Repression in Iran. Netherlands. Available from: http://giswatch.org/sites/default/files/gisw_-_iran.pdf [Accessed 11 September 2013]

- Global Innovation Index (2013) The Local Dynamics of Innovation. *Cornell University, INSEAD, and WIPO*. Published 5 July 2013. Available from: <http://odessablog.files.wordpress.com/2013/07/gii-2013.pdf> [Accessed 22 October 2013]
- Global Mail (2012) Iran: Not Tweeting, Hacking. *Digital Global Mail Ltd*. Published 2 April 2012. Available from: <http://www.theglobalmail.org/feature/iran-not-tweeting-hacking/165> [Accessed 10 December 2013]
- Global Times (2012) Iranians in Defiance of Outside Pressures Amid Economic Woes. Available from: <http://mobile.globaltimes.cn/content/697564.html> [Accessed 1 October 2013]
- Global Voices (2007) Iran: Flickr Users vs. The State. Published 14 February 2007. Available from: <http://globalvoicesonline.org/2007/02/14/access-flickr-iran> [Accessed 17 September 2013]
- Global Voices (2010) Iran: Campaign to Free Jailed Photo-Blogger Hamed Saber. Published 27 July 2010. Available from: <http://advocacy.globalvoicesonline.org/2010/07/27/iran-campaign-to-free-jailed-photo-blogger-hamed-saber> [Accessed 18 September 2013]
- Globe and Mail (2013) After Weeks of Negotiations, EU Blames Canada for Stalled Trade Deal. *The Globe and Mail Inc*. Published 18 June 2013. Available from: <http://www.theglobeandmail.com/news/politics/eu-says-its-been-waiting-for-canada-to-make-compromises-on-trade-deal/article12636160> [Accessed 7 October 2013]
- Golafshani, N. (2003) Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*. **8**(4): 597–607
- Golding, P. (2000) Forthcoming Features: Information and Communications Technologies and the Sociology of the Future. *Sociology*. **34**(1): 165–184
- Goldstein, J. (2007) The Role of Digital Networked Technologies in the Ukrainian Orange Revolution. *Internet and Democracy Case Study 2007-14*. Berkman Centre for Internet and Society at Harvard University. Cambridge, MA, USA. Available from: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf [Accessed 10 July 2011]
- Golkar, S. (2011) Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran. *International Journal of Emerging Technologies and Society*. **9**(1): 50–70
- Google Online Security (2011) An Update on Attempted Man-in-the-middle Attacks. *Google Inc*. Published 29 August 2011. Available from: <http://googleonlinesecurity.blogspot.co.uk/2011/08/update-on-attempted-man-in-middle.html> [Accessed 1 October 2013]
- Gounari, P. and Grollios, G. (2010) New Information and Communication Technologies as Spaces for Critical Literacy. *Proceedings, 4th International Technology, Education and Development Conference*. Valencia, Spain. Held 8–10 March 2010. pp. 3097–104

- Gratton, L. (2010) The Future of Work. *Business Strategy Review*. **21**(3): 16–23
- Green Voice of Freedom (2010) Who are the Iranian Cyber Army? Available from: <http://en.irangreenvoice.com/article/2010/feb/19/1236> [Accessed 14 July 2011]
- Greene, S. (1995) A Functional Approach to Documentation and Metadata. *IASSIST Quarterly*. **19**(3): 16–21
- Greenwood, D.J. (2008) Theoretical Research, Applied Research and Action Research. In: C.R. Hale (Ed.) *Engaging Contradictions: Theory, Politics and Methods of Activist Scholarship*: 319–40
- GTZ (2008) Promoting Economic Innovations in Sub-Sahara Africa. *Deutsche Gesellschaft für Technische Zusammenarbeit GmbH*. Published 16 March 2009. Bonn, Germany. Available from: http://www2.gtz.de/wbf/4tDx9kw63gma/Promoting_Economic_Innovations.pdf [Accessed 18 October 2013]
- Gu, S., Liu, J., Lundvall, B.Å. and Schwaag-Serger, S. (2008) China's System and Vision of Innovation: Analysis of the National Medium and Long-Term Science and Technology Development Plan (2006-2020)
- Gu, S. and Steinmueller, W.E. (1997) China's National Innovation System Approach to Participating in Information Technology: The Innovative Recombination of Technological Capability. *Institute of New Technologies, United Nations University*. Shibuya, Tokyo, Japan
- Guan, J.C., Yam, R., Tang, E.P. and Lau, A.K. (2009) Innovation Strategy and Performance During Economic Transition: Evidences in Beijing, China. *Research Policy*. **38**(5): 802–12
- Guardian (2010) LimeWire Shut Down by Federal Court. *Guardian News and Media Ltd*. Published 27 October 2010. Available from: <http://www.theguardian.com/technology/2010/oct/27/limewire-shut-down> [Accessed 21 September 2013]
- Guion, L.A., Diehl, D.C. and McDonald, D. (2011) Triangulation: Establishing the Validity of Qualitative Studies. *University of Florida IFAS Extension, Publication No. FCS6014*. Gainesville, FL, USA
- Gummett, P. and Stein, J.A. (1997) European Defence Technology in Transition. London, UK: *Routledge*
- Gunduz, H.B. (2010) Digital Divide in Turkish Primary Schools: Sakarya Sample. *Turkish Online Journal of Educational Technology*. **9**(1): 43–53
- Habermas, J. (1989) The Structural Transformation of the Public Sphere. Cambridge, UK: MIT Press
- Habermas, J. (1994) Three Normative Models of Democracy. *Constellations*. **1**(1): 1–10

Habermas, J. (1996) *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge, MA, USA: *The MIT Press*

Habermas, J. (2003) The Post-National Constellation. In: David Held and Anthony McGrew (Eds.) *The Global Transformations Reader: An Introduction to the Globalization Debate*. Cambridge, UK: Polity Press

Habermas, J. (2006) Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research. *Communication Theory*. **16**(4): 411–26

Haghi, S.R., Sabahi, A. and Salnazaryan, A. (2011) Institution and Functions of National Innovation System in Norway and Iran. *African Journal of Business Management*. **5**(24): 10108–16

Hakakian, R. (2012) Where did Iran's Green Movement Go? *The New York Times*. Published Sunday, 1 April 2012: p. 2

Hale, C.R. (2008) *Engaging Contradictions: Theory, Politics and Methods of Activist Scholarship*. Oakland, CA, USA: *University of California Press*

HAMSA (2007) Spotlight Cases: Facebook Faces Censorship in Iran. *Civil Rights in the Middle East*. Available from: <http://www.hamsaweb.org/crime/4.html> [Accessed 26 November 2013]

Hamshahri Online (2011) Is Using VPNs Illegal [in Iran]? Published 12 October 2011. Tehran, Iran. Available from: <http://hamshahrionline.ir/details/148264> [Accessed 10 September 2013]

Hammersley, M. (2008) Troubles with Triangulation. In: M.M. Bergman (Ed.) *Advances in Mixed Methods Research*. pp. 22–36. London, UK: SAGE Publications Ltd.

Harasymiw, B. (2007) Ukraine's Orange Revolution and Why it Fizzled. *Paper prepared for presentation to the annual meeting of the Canadian Political Science Association at the 76th Congress of the Humanities and Social Sciences, University of Saskatchewan*. Presented 1 June 2007. Saskatoon, SK, Canada

Haraway, D.J. (1994) A Game of Cat's Cradle: Science Studies, Feminist Theory and Cultural Studies. *Configurations*. **2**(1): 59–71

Hargreaves, J. (2009) From Voice to Dialogue to *Connect*. **175**: 19–21. Melbourne, Victoria, Australia: Royal Melbourne Institute of Technology (RMIT)

Hasse, C. (2011) Profile: Professor Cathrine Hasse. *School of Education, University of Stirling, Stirling, UK*. Available from: <http://www.propel.stir.ac.uk/people/profiles/cathrine-hasse.php> [Accessed 1 October 2013]

Hastedt, G., Shannon, V.P. and Lybecker, D.L. (2014) *Cases in International Relations: Pathways to Conflict and Cooperation*. Thousand Oaks, CA, USA: *SAGE Publications Ltd*.

- Heap, A. (2010) Anti-Censorship Software Licensed by US Government for Export to Iran. Available from: <http://blog.austinheap.com/anti-censorship-software-licensed-by-us-government-for-export-to-iran> [Accessed 20 April 2011]
- Hearn, K., Mahneke, R.J. and Williams, P.A. (2009) Culture Jamming: From Activism to Hactivism. *Edith Cowan University*. Perth, Australia. Available from: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1002andcontext=isw> [Accessed 20 April 2011]
- Heideman, K. (2009) Women in the Iranian Election Campaign and Protest. *Middle East Program, Woodrow Wilson International Centre for Scholars*. Occasional Paper Series. Published Fall 2009. Washington DC, USA
- Herrmann, D.J. and Raybeck, D. (1996) A Clash of Cultures: Basic and Applied Cognitive Research. In: D.G. Payne and F.G. Conrad (Eds.) *Intersections in Basic and Applied Memory Research*. Mahwah, NJ, USA: Erlbaum
- Herstad, S., Pålshaugen, Ø. and Ebersberger, B. (2011) Industrial Innovation Behaviour in a Capital Region Context. Published 9 January 2011. Available from: http://www.berndebersberger.com/wp-content/uploads/2011/01/capital_region_v6.pdf [Accessed 12 October 2013]
- Higgins, A. (2010) Revolutionary Guard Inc. *CrethiPlethi.com*. Published 8 February 2010. Available from: <http://www.crethiplethi.com/revolutionary-guard-inc/islamic-countries/iran-islamic-countries/2010> [Accessed 09 September 2013]
- Hine, C. (2007) Multi-Sited Ethnography as a Middle Range Methodology for Contemporary STS. *Science, Technology and Human Values*. **32**(6): 652–71
- Hine, C. (2011) Towards Ethnography of Television on the Internet: A Mobile Strategy for Exploring Mundane Interpretive Activities. *Media, Culture and Society*. **33**(4): 567–82
- Hintz, A. (2012) Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring. *ESSACHESS Journal for Communication Studies*. **5**(1): 83–105
- Hoghooghhdanan (2011) The Legal Debate over the Use of VPNs. Published 18 October 2011. Available from: http://www.hoghooghhdanan.com/index.php?option=com_contentandview=articleandid=2472:-----lvpnrandcatid=56:cyberandItemid=73 [Accessed 10 September 2013]
- Holmes, B. (2007) Continental Drift: Activist Research, from Geo-Politics to Geo-Poetics. *Constituent Imagination: Militant Investigations, Collective Theorisation*: 39-43
- Honigsheim, P. (2003) The Unknown Max Weber. New Jersey, USA: *Transaction Books*
- Howard, P.N., Agarwal, S.D. and Hussain, M.M. (2011) When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media. *The Communication Review*. **14**(3): 216–32

Hox, J.J. and Boeijs, H.R. (2005) Data Collection: Primary vs. Secondary. *Encyclopaedia of Social Measurement*. **1**: 593–99

HRANA (2013) Two Facebook Users were Arrested by FATA Police. *Human Rights Activists News Agency*. Published 15 July 2013. Available from: <https://hra-news.org/en/two-facebook-users-were-arrested-by-fata-police> [Accessed 18 September 2013]

Hrycak, A. and Rewakowicz, M.G. (2009) Feminism, Intellectuals and the Formation of Micro-Publics in Post Communist Ukraine. *Formerly Studies in Soviet Thought*. **61**(4): 310–33

Hrycak, A. (2010) Orange Harvest?: Women's Activism and Civil Society in Ukraine, Belarus and Russia since 2004. *Canadian-American Slavic Studies*. **44**: 151–77

Huffington Post. (2012) World Happiness Report 2012: Scandinavian Countries Are Happiest on Earth. *The Huffington Post Inc.* Published 06 April 2012. Available from: http://www.huffingtonpost.com/2012/04/06/world-happiness-report-2012_n_1408787.html [Accessed 19 September 2013]

Hussein, A. (2009) The Use of Triangulation in Social Sciences Research: Can Qualitative and Quantitative Methods be Combined? *Journal of Comparative Social Work*. **1**(8): 1–12

Huyer, S. and Mitter, S. (2003) ICTs, Globalisation and Poverty Reduction: Gender Dimensions of the Knowledge Society. Kampala, Uganda: *Comisión de Ciencia y Tecnología para el Desarrollo (Naciones Unidas), Junta Consultiva sobre Cuestiones de Género*.

Ikejiaku, B.V. (2014) International Law is Western-Made Global Law: The Perception of Third-World Category. *African Journal of Legal Studies*. **6**(2/3): 337–56

Indymedia (2010) Iranian Expatriates in America: The New House Negroes? Published 9 February 2010. Available from: <http://www.indymedia.org.uk/en/regions/world/2010/02/445903.html> [Accessed 2 October 2013]

Inglehart, R., Norris, P. and Welzel, C. (2002) Gender Equality and Democracy. *Institute for Social Research, University of Michigan*. MI, USA. Available from: <http://wiki.zirve.edu.tr/sandbox/groups/economicsandadministrativesciences/wiki/37a80/attachments/88853/Week9-Inglehartetal.pdf> [Accessed 4 October 2013]

Intarakumnerd, P., Chairatana, P.A. and Tangchitpiboon, T. (2002) National Innovation System in Less Successful Developing Countries: The Case of Thailand. *Research Policy*. **31**(8): 1445–57

Institute for International Economics (2006a) The Exon-Florio Amendment. Published 19 April 2006. Available from: http://www.iie.com/publications/chapters_preview/3918/02iie3918.pdf [Accessed 12 October 2013]

Institute for International Economics (2006b) Globalisation of Innovation. Published 12 June 2006. Available from: http://www.iie.com/publications/chapters_preview/3900/06iie3900.pdf [Accessed 18 October 2013]

Institute for Middle East Studies (2011) Iran in Transition. *Annual Conference Held on 21 April 2011 at Elliott School of International Affairs, George Washington University*. Washington DC, USA. Available from: <http://www.gwu.edu/~imes/assets/Iran%20In%20Transition.pdf> [Accessed 2 November 2013]

International Business Times (2012) The Surprising Truth about Internet Censorship in the Middle East. *IBT Media Inc*. Published 12 October 2012. Available from: <http://www.ibtimes.com/surprising-truth-about-internet-censorship-middle-east-845933> [Accessed 7 December 2013]

International Business Times (2013) Cyber-Rebels See Way to Get Around Iran's VPN Internet Block. *IBT Media Inc*. Published 11 March 2013. Available from: <http://www.ibtimes.com/cyber-rebels-see-way-get-around-irans-vpn-internet-block-1118671> [Accessed 16 September 2013]

International Relations Review (2013) The Revolution Will not be Televised: Youth, Gender and Islam in Iran. Published 16 April 2013. Available from: <http://irr.buiaa.org/2013/04/the-revolution-will-not-be-televised-youth-gender-and-islam-in-iran> [Accessed 20 September 2013]

International Renaissance Foundation and Stefan Batory Foundation (2010) Beyond Colours: Assets and Liabilities of Post-Orange Ukraine. Published 30 April 2010. Available from: <http://www.irf.ua/files/ukr/beyond%20colours.pdf> [Accessed 15 October 2013]

Internet and Democracy Blog (2008) Understanding the Iranian Blogosphere. *Berkman Centre for Internet and Society at Harvard Law School, Harvard University*. Published 11 January 2008. Cambridge, MA, USA. Available from: <https://blogs.law.harvard.edu/idblog/2008/01/11/understanding-the-iranian-blogosphere> [Accessed 12 September 2013]

Iran Media Program. (2012) Persian Cyberspace Report: Internet Blackouts across Iran; BBC Journalists Interrogated, Family Members Imprisoned. *Annenberg School of Communications, University of Pennsylvania*. Published 9 February 2012. Philadelphia, PA, USA. Available from: <http://iranmediaresearch.com/en/blog/101/12/02/09/840> [Accessed 17 September 2013]

Iranian Embassy in Norway (2011) Student Advisory: Education System in Iran. Oslo, Norway. Available from: <http://www.iran-embassy-oslo.no/embassy/educat.htm> [Accessed 4 December 2013]

Iran Watch (2013) Baghyatollah Medical Sciences University. *Wisconsin Project on Nuclear Arms Control*. Published 24 July 2013. Available from: <http://www.iranwatch.org/iranian-entities/baghyatollah-medical-sciences-university> [Accessed 2 November 2013]

- iRevolution (2012) Innovation and Counter-Innovation: Digital Resistance in Russia. *iRevolution*. Published 9 March 2012. Available from: <http://irevolution.net/2012/03/09/digital-resistance-in-russia> [Accessed 1 October 2013]
- Irwin, D.A. (1996) The US-Japan Semiconductor Trade Conflict. Chicago, USA: *University of Chicago Press*. Published 30 November 2007. Available from: <http://www.nber.org/chapters/c8717.pdf> [Accessed 12 October 2013]
- Isakow, R. (2011) Revolutionary Iranian Corruption. *Financial Transparency Coalition, Centre for International Policy*. Published 28 June 2011. Available from: <http://www.financialtransparency.org/2011/06/28/revolutionary-iranian-corruption> [Accessed 18 December 2013]
- Ishizuka, M. and Matsuda, T. (1990) Knowledge Acquisition Mechanisms for a Logical Knowledge Base Including Hypotheses. *Knowledge-Based Systems*. **3**(2): 77–86
- Jackson, T. (2012) Sorting the Indigenous from the Endogenous in Cross-Cultural Management Research. *Middlesex University Business School*. Published 27 July 2012. Available from: <http://terencejackson.net/2012/07/27/sorting-the-indigenous-from-the-endogenous-in-cross-cultural-management-research> [Accessed 30 July 2015]
- Jasanoff, S. (2003) Breaking the Waves in Science Studies: Comment on H.M. Collins and R. Evans' "The Third Wave of Science Studies". *Social Studies of Science*: 389–400
- Jensen, H.S., Richter, L.M. and Vendel, M.T. (2003) The Evolution of Scientific Knowledge. *Edward Elgar Publishing*. Cheltenham, UK
- Jerusalem Post (2011) Iran Embarks on \$1b Cyber-warfare Program. Published 18 December 2011. Available from: <http://www.jpost.com/Defense/Iran-embarks-on-1b-cyber-warfare-program> [Accessed 1 October 2013]
- Jick, T.D. (1979) Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*. **24**(4): 602–11
- Johnson, B., Edquist, C. and Lundvall, B.Å. (2004) Economic Development and the National System of Innovation Approach. *Paper Presented at the First Globelics Conference, 3–6 November 2003, Rio de Janeiro, Brazil*
- Jørgensen, K.E. (2006) A Multilateralist Role for the EU? In: O. Elgström and M. Smith (Eds.) *The European Union's Roles in International Politics: Concepts and Analysis*. Routledge: Abingdon, Oxon, UK
- Jørgensen, K.E. (2013) The State of EU Foreign Policy: Constituting a Global Player. *Approaching the European Federation?* p. 165
- Joudeh, R. (2011) Egypt: A Social Network Revolution with a Twist. *The Moscow News*. Published 1 February 2011. Available from: <http://themoscownews.com/comments/20110201/188383255.html> [Accessed 3 December 2013]

- Joyce, M. (2011) A New Framework for Digital Activism and Digital Repression. *Meta Activism*. Available from: <http://www.meta-activism.org/2011/02/digital-activism-and-repression-framework> [Accessed 6 February 2013]
- Kaeding, M. and Voskamp, F. (2011) Better Implementation of EU Legislation Isn't Just a Question of Taking Member States to Court. *European Institute of Public Administration working paper 2011/W/01*. Available from: http://www.eipa.eu/files/repository/product/20120228091739_Workingpaper2011_W_01.pdf [Accessed 7 October 2013]
- Kalathil, S. and Boas, T.C. (2003) Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. *Carnegie Endowment for International Peace*. Washington DC, USA: *The Brookings Institution Press*
- Kanamori, T., Lim, J.J. and Yang, T. (2007) China's SME Development Strategies in the Context of a National Innovation System. *Asian Development Bank Institute (ADB) Discussion Paper 55*
- Kanwar, A. (2009) Rending the Veil: Women Challenging the Theocracy. *International Journal of the Humanities*. **6**(9): 53–60
- Kaplan, R.D. (2006) Cultivating Loneliness: The Importance of Slipping Away from the Pack to Encounter and Understand the World First-Hand. *Columbia Journalism Review*. **44**(5): 48–52
- Karatnycky, A. (2005) Ukraine's Orange Revolution. *Foreign Affairs*. March–April 2005. **84**(2): 35–52
- Karatzogianni, A. (2013) A Cyber-Conflict Analysis of the 2011 Arab Spring Uprisings. In: Youngs, G. (Ed.) *Digital World: Connectivity, Creativity and Rights*. Published July 2013. London and New York: Routledge
- Karlekar, K.D. and Cook, S.G. (2009) Access and Control: A growing Diversity of Threats to Internet Freedom. *Freedom House*. Washington DC, USA. Available from: <http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FOTN%20Overview%20Essay.pdf> [Accessed 20 April 2011]
- Kelly, J. and Etling, B. (2008) Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere. *Berkman Centre for Internet and Society at Harvard Law School*. Harvard University. Cambridge, MA, USA. Available from: http://www.academia.edu/download/30532165/mapping_irans_online_public_-_pdf_-_english.pdf [Accessed 01 July 2014]
- Kelly-Garrett, R. (2006) Protest in an Information Society: A Review of Literature on Social Movements and New ICTs. *Information, Communication and Society*. **9**(2): 202–24

Khamis, S., Gold, P.B. and Vaughn, K. (2012) Beyond Egypt's Facebook Revolution and Syria's YouTube Uprising: Comparing Political Contexts, Actors and Communication Strategies. *University of Maryland, College Park*. MD, USA. Available from: http://www.arabmediasociety.com/articles/downloads/20120407120519_Khamis_Gold_Vaughn.pdf [Accessed 21 January 2013]

King, G., Pan, J. and Roberts, M.E. (2013) How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*. **107**(2): 326–43

Kinkel, S., Lichtner, R., Hochdörffer, J. and Ruhrmann, S. (2015) Fields and Patterns of German Companies' Operation and Collaboration Strategies in China. *Presented in June 2015 at the 22nd International Annual EurOMA Conference*. Neuchâtel, Switzerland

Klasen, S. (2002) Does Gender Inequality in Education Reduce Growth and Development? Evidence from Cross-Country Regressions. *World Bank Economic Review*. **16**: 345–73. Oxford, UK: Oxford University Press

Knapp, K.J. and Boulton, W.R. (2006) Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. *Information Systems Management*. Spring: 76–87

Kojoori-Saatchi, A.E. (2010) The Culture of Revolution: Revolutionary Transformation in Iran. *University of Nevada, Las Vegas*. NV, USA. Available from: <http://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1815&context=thesesdissertations> [Accessed 6 August 2012]

Kortunov, V.V. and Platonova, N.A. (2013) Philosophical and Socio-Cultural Aspects of the Economic Type of Thinking. *Middle East Journal of Scientific Research*. **16**(2): 296–303

Kulve, H.T. and Smit, W.A. (2003) Civilian-military Co-operation Strategies in Developing New Technologies. *Research Policy*. **32**(6): 955–70

Kuper, A., Lingard, L. and Levinson, W. (2008) Critically Appraising Qualitative Research. *BMJ*. Published 20 Sep 2008. **337**: 687–92

Kurzman, C. (2012) The Arab Spring: Ideals of the Iranian Green Movement, Methods of the Iranian Revolution. *International Journal of Middle East Studies*. Published February 2012. **44**(1): 162–65

Kuzio, T. (2005a) Revisiting the Orange Revolution: Considerable Gains Made. *Eurasia Daily Monitor*. Published Monday, 21 November 2005. Washington DC, USA: *Jamestown Foundation*

Kuzio, T. (2005b) Ukraine's Orange Revolution: The Opposition's Road to Success. *Journal of Democracy*. April 2005. **16**(2): 117–30

Kuzio, T. (2006) Everyday Ukrainians and the Orange Revolution. In: Anders Aslund and Michael McFaul (Eds.) *Revolution in Orange*. Carnegie Endowment. Washington DC, USA. pp. 45–68

Kuzio, T. (2008) Ukrainian Politics, Energy and Corruption under Kuchma and Yushchenko: How the Gas Issue Plays in Ukrainian Politics and How Ukrainian Politicians Play the Gas Issue. *Harvard University*. Published 7 March 2008. Cambridge, Massachusetts, USA. Available from: http://www.taraskuzio.net/conferences2_files/Ukrainian_Politics_Energy.pdf [Accessed 22 October 2013]

Kwon, K.S. (2010) Universities' Academic Research and Knowledge-Transfer Activities in a Catch-up Country: The Case of Korea. *Doctoral Dissertation*. University of Sussex. Sussex, UK

Kyj, M.J. (2006) Internet Use in Ukraine's Orange Revolution. *Business Horizons*. **49**: 71–80. *Kelley School of Business, Indiana University*. Indiana, USA

La Pastina, A.C. (2006) The Implications of an Ethnographer's Sexuality. *Qualitative Inquiry*. **12**(4): 724–35

LA Times (2012) Iranian Universities Shut Female Students Out of Dozens of Fields. *Los Angeles Times*. Published 20 August 2012. Los Angeles, CA, USA. Available from: http://latimesblogs.latimes.com/world_now/2012/08/iranian-universities-female-students.html [Accessed 6 October 2013]

LaPier, T. (1998) Competition, Growth Strategies and the Globalisation of Services. NY, USA: *Routledge*

Laskowska, M. (2014) Social Networking Services in Service of Democracy: Chosen Case Studies. *Online Journal of Communication and Media Technologies*. **4**(1)

Leberknight, C.S., Chiang, M., Poor, H.V. and Wong, F. (2010) A Taxonomy of Internet Censorship and Anti-Censorship. *Princeton University*. NJ, USA. Available from: <http://www.princeton.edu/~chiangm/anticensorship.pdf> [Accessed 20 April 2011]

Lederer, N. and Ernest, D.J. (2000) Media Reports a Library Disaster: A Case Study at Colorado State University. *Colorado State University Libraries*. Fort Collins, Colorado, USA

Lewkowicz, M. and Rohde, M. (2011) Socially Embedded Collaborative Practices: Introduction to a Special Issue based on the COOP 2010 Conference. *Computer-Supported Cooperative Work*. **20**(4): 227–29

Leydesdorff, L. and Guoping, Z. (2001) University-Industry-Government Relations in China: An Emergent National System of Innovation. *Industry and Higher Education*. **15**(3): 179–82

Li, J., Casey, C. and Brewer, L.K. (2015) Exploring Opportunities for Engaging Public Health Organisations in Transportation Planning. *Public Works Management and Policy*: 1087724X14559520. USA: University of Texas at Arlington

Lieberson, S. (1989) When Right Results Are Wrong. *Society*. **26**(5): 60–6

Lievrouw, L.A. (2004) What has Changed about New Media? Introduction to the Fifth Anniversary Issue of New Media and Society. *New Media and Society*. **6**(1): 9–15. London, UK: *SAGE Publications Ltd*.

- Lins-Ribeiro, G. (2013) Global Flows of Development Models. *Anthropological Forum*. **23**(2): 121–41. London / New York: Routledge
- List, F. (1841) The National System of Political Economy. English Edition (1904). London, UK: *Longman*
- Livingstone, S. (2003) The Changing Nature and Uses of Media Literacy. *Media@LSE Electronic Working Paper 4*. London School of Economics and Political Science. London, UK
- Livingstone, S. (2004) Media Literacy and the Challenge of New Information and Communication Technologies. *The Communication Review*. **7**(1): 3–14
- Liu, X. and Lundin, N. (2007) Toward a Market-Based Open Innovation System of China. *Graduate University of Chinese Academy of Science*. Beijing, China
- Liu, X. and White, S. (2001) Comparing Innovation Systems: A Framework and Application to China's Transitional Context. *Research Policy*. **30**(7): 1091–1114
- Lock, R., Cooke, L. and Jackson, T. (2013) Online Social Networking: Order and Disorder. *The Electronic Journal of E-Government (EJEG)*. **11**(1): 229–40. Kidmore End, Reading, UK: Academic Publishing International Ltd.
- Lu, Y. (2001) Construction of Chinese National S&T Innovation System and Latest Advancements in Science and Technology in China. *Current Science*. **81**(8): 930–35
- Luehrmann, L. (2007) Comparative Politics of the Third World: Linking Concepts and Cases. Second Edition. Boulder, CO, USA: *Lynne Rienner Publishers*
- Lundvall, B.Å. (1985) Product Innovation and User-Producer Interaction. *Industrial Development Research Series No. 31*, Aalborg University Press. Aalborg, Denmark
- Lundvall, B.Å. (1992). National Innovation Systems: Towards a Theory of Innovation and Interactive Learning. London: *Pinter*
- Lundvall, B.Å. (1995) The Learning Economy: Challenges to Economic Theory and Policy. *Universite Louis Pasteur*. Strasbourg, Alsace, France
- Lundvall, B.Å., Johnson, B., Andersen, E.S. and Dalum, B. (2002) National Systems of Production, Innovation and Competence Building. *Research Policy*. **31**(2): 213–31
- Lutsevych, O. (2013) How to Finish a Revolution: Civil Society and Democracy in Georgia, Moldova and Ukraine. *Chatham House*. Briefing Paper REP BP 2013/01. Published January 2013. London, UK. Available from: http://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0113bp_lutsevych.pdf [Accessed 15 October 2013]
- Lyasnikov, N.V.E., Dudin, M.N., Sekerin, V.D., Veselovsky, M.Y. and Aleksakhina, V. G. (2014) The National Innovation System: The Conditions of its Making and Factors in its Development. *Life Science Journal*. **11**(6): 535–38

- Lynch, M. and Cole, S. (2005) Science and Technology Studies on Trial: Dilemmas of Expertise. *Social Studies of Science*. **35**(2): 269–311
- Lysenko, V.V. and Desouza K.C. (2010) The Role of Internet-based Information Flows and Technologies in Electoral Revolutions: The Case of Ukraine's Orange Revolution. *First Monday*. Published 6 September 2010. **15**(9)
- MacKenzie, D. and Wajcman, J. (1985) *The Social Shaping of Technology: How the Refrigerator Got Its Hum*. Milton Keynes, Buckingham, UK: *Open University Press*
- MacKenzie, D. and Wajcman, J. (1999) *The Social Shaping of Technology*. Second Edition. Milton Keynes, Buckingham, UK: *Open University Press*
- Magaudda, P. (2014) The Broken Boundaries between Science and Technology Studies and Cultural Sociology: Introduction to an Interview with Trevor Pinch. *Cultural Sociology*. **8**(1): 63–76
- Magone, J.M. (2006) *The New World Architecture: The Role of the European Union in the Making of Global Governance*. NJ, USA: *Transaction Books*
- Mail and Guardian (2013) US Trial Turns Heat on MTN. *Mail and Guardian Online*. Published 15 February 2013. Available from: <http://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn> [Accessed 17 September 2013]
- Majlis (2011) 25 Articles of the Cyber Crime Law Were Passed by the Parliament. Tehran, Iran. Available from: <http://tarh.majlis.ir/?ShowNewsandId=28> [Accessed 19 July 2011]
- Maleki, A., Packniat, M., Barkhordar, B. and Moghaddas-Kelishomi, A. (2005) Developing Innovation Policies for Telecom Sector in Islamic Republic of Iran. *GLOBELICS Conference on Innovation Systems Promoting Economic Growth, Social Cohesion and Good Governance*. 31 October–4 November 2005. Tshwane University of Technology. Pretoria, South Africa
- Malerba, F. and Breschi, S. (1997) Sectoral Innovation Systems. In: C. Edquist (Ed.) *Systems of Innovation*. London, UK: Edgar
- Malmberg, A. and Maskell, P. (1997) Towards an Explanation of Regional Specialisation and Industry Agglomeration. *European Planning Studies*. **5**(1): 25–41
- Mani, S. (2004) A National System of Innovation in the Making: An Analysis of the Role of Government with Respect to Promoting Domestic Innovations in the Manufacturing Sector of Iran. *Institute for New Technologies, United Nations University*. Tokyo, Japan. Available from: <http://www.intech.unu.edu/publications/discussion-papers/2004-12.pdf> [Accessed 5 September 2011]
- Mansell, R. (1999) Information and Communication Technologies for Development: Assessing the Potential and the Risks. *Telecommunications Policy*. **23**(1): 35–50

Mashregh News (2012) Who Is Smarter: Internet Users or Filtering Officials? Published 7 February 2012. Tehran, Iran. Available from:
<http://www.mashreghnews.ir/fa/news/94916/کاربران-اینترنت-باهوش-ترند-یا-مسئولین-فیلترینگ/>
[Accessed 10 September 2013]

Masoud, E. (2006) Islam and Science: An Islamist Revolution. *Nature*. **444**: 22–25.
Published 2 November 2006

Masson, H., Balfe, M., Hackett, S. and Phillips, J. (2013) Lost without a Trace? Social Networking and Social Research with a Hard-to-Reach Population. *British Journal of Social Work*. **43**(1): 24–40

Mathews, J.A. (1999) From National Innovation Systems to National Systems of Economic Learning: The Case of Technology Diffusion Management in East Asia. *Paper submitted to DRUID Summer Conference*. Presented June 1999. Rebuild, Denmark

Mathison, S. (1988) Why Triangulate? *Educational Researcher*. **17**(2): 13–17

May, T. (1999) Reflexivity and Sociological Practice. *Sociological Research Online*. Department of Sociology, University of Surrey. Guildford, UK

Maxey, I. (1999) Beyond Boundaries? Activism, Academia, Reflexivity and Research. *Area*. **31**(3): 199–208

McClatchy DC (2009) Iran's Senior Ayatollah Slams Election, Confirming Split. *McClatchy Newspapers*. Published 16 June 2009. Sacramento, California, USA. Available from:
<http://www.mcclatchydc.com/2009/06/16/70155/irans-senior-ayatollah-slams-election.html>
[Accessed 8 December 2013]

McFaul, M. (2007) Ukraine Imports Democracy: External Influences on the Orange Revolution. *International Security*. Fall 2007. **32**(2): 45–83

McLuhan, M. (1962) *The Gutenberg Galaxy: The Making of Typographic Man*. Toronto, Canada: *University of Toronto Press*

Mehriran (2010) Activities of the IRGC to Tackle 'Soft' Threats. *Mehriran*. Published 21 May 2010. Tehran, Iran. Available from: <http://www.mehriran.de/en/articles/single/datum///activities-of-the-irgc-to-tackle-soft-threats> [Accessed 11 September 2013]

Mejias, U.A. (2012) Liberation Technology and the Arab Spring: From Utopia to Atopia and Beyond. *Fibre-Culture Journal (FCJ-147)*: 214–17

Menon, N. (2015) Fighting Patriarchy and Capitalism. *Journal of Contemporary African Studies*. **33**(1): 3–11

Merton, R.K. (1936) The Unanticipated Consequences of Purposive Social Action. *American Sociological Review*. **1**(6): 894–904

Metghalchi, N. (2011) Is Iran Immune from the Arab Spring? *FRIDE*. Policy Brief (ISSN: 1989 - 2667). Number 99. Published October 2011

Miao, C.H., Wei, Y.D. and Ma, H. (2007) Technological Learning and Innovation in China in the Context of Globalisation. *Eurasian Geography and Economics*. **48**(6): 713–32

Milani, A. (2010) The Green Movement. *The Iran Primer: Power, Politics and US Policy*. United States Institute of Peace (USIP). Washington DC, USA

Military Advantage (2008) Iranian Cyber Warfare Threat Assessment. *Defence Tech*. Published 23 September 2008. Available from: <http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment> [Accessed 10 December 2013]

Minogue, M. (2001) The Internationalisation of New Public Management. In: W. McCourt and M. Minogue (Eds). *The Internationalisation of Public Management: Reinventing the Third World State*. Northampton, UK: Edward Elgar

Mishkova, D. (2012) Liberalism and Tradition in the Nineteenth-Century Balkans: Toward History and Methodology of Political Transfer. *Centre for Advanced Study*. Published 6 September 2012. Sofia, Bulgaria. Available from: <http://eep.sagepub.com/content/early/2012/09/04/0888325412459310> [Accessed 17 October 2013]

MIT Technology Review (2009a) The Web vs. the Republic of Iran. *Massachusetts Institute of Technology*. Published 18 June 2009. Cambridge, MA, USA. Available from: <http://www.technologyreview.com/news/413903/the-web-vs-the-republic-of-iran> [Accessed 10 September 2013]

MIT Technology Review (2009b) Why Twitter Doesn't Mean the End of Iranian Censorship. *Massachusetts Institute of Technology*. Published 16 June 2009. Cambridge, MA, USA. Available from: <http://www.technologyreview.com/view/413881/why-twitter-doesnt-mean-the-end-of-iranian-censorship> [Accessed 10 September 2013]

Mohan, B. (2011) Development, Poverty of Culture, and Social Policy. Hampshire, UK: Palgrave Macmillan

Moore, H.L. and Selchow, S. (2012) Global Civil Society and the Internet 2012: Time to Update Our Perspective. In: M. Kaldor, H.L. Moore and S. Selchow (Eds.) *Global Civil Society 2012: Ten Years of Critical Reflection*. Part i, Chapter ii: 28–40

Moran-Ellis, J., Alexander, V.D., Cronin, A., Dickinson, M., Fielding, J., Sleney, J. and Thomas, H. (2006) Triangulation and Integration: Processes, Claims and Implications. *Qualitative Research*. **6**(1): 45–59

Morgan, J. (2006) Issues in the Political Economy of Economic Transition in the Peoples' Republic of China. *The Centre of Excellence in Global Governance Research, University of Helsinki*. Working paper 1. Helsinki, Finland

Morse, J.M. (2006) The Politics of Evidence. *Qualitative Health Research*. **16**(3): 395–404

Motohashi, K. and Yun, X. (2007) China's Innovation System Reform, Growing Industry and Science Linkages. *Research Policy*. **36**(8): 1251–60

Mueller, P.S. and Van Huellen, S. (2012) A Revolution in 140 Characters? Reflecting on the Role of Social Networking Technologies in the 2009 Iranian Post-Election Protests. *Policy and Internet*. **4**(3–4): 184–205

Muftah (2010) The State of Iran's Economy: An Interview with Professor Kaveh Ehsani. Published 15 October 2010. Available from: <http://muftah.org/the-state-of-iran's-economy-an-interview-with-professor-kaveh-ehsani> [Accessed 1 October 2013]

Mussuri, Y.A. (2005) Foreign Aid to the Media in Ukraine and its Impact on the Democratisation Process in the Country. *University of Georgia*. Athens, GA, USA. Available from: http://athenaeum.libs.uga.edu/bitstream/handle/10724/8570/mussuri_yevgeniya_a_200508_ma.pdf?sequence=1 [Accessed on 6 August 2012]

Myerson, R.B. (1991) Game Theory: Analysis of Conflict. MA, USA: *Harvard University Press*

Naghdi, A. (2010) Iranian Diaspora: With Focus on Iranian Immigrants in Sweden. *Asian Social Science*. Published November 2010. **6**(11): 197–208

Nambiar, M. and Kennedy, S.H. (2012) Organisational Excellence through Innovation Management. In: M.S. Rangaraju and S.H. Kennedy (Eds.) *Innovation in Management Challenges and Opportunities in the Next Decade*: 97–109

Nawaat (2010) The Internet Freedom Fallacy and the Arab Digital Activism. *Nawaat*. Published 17 September 2010. Available from: <http://nawaat.org/portail/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism> [Accessed 17 September 2013]

Nazario, J. (2009) Politically Motivated Denial of Service Attacks. *Arbour Networks*. Chelmsford, MA, USA. Available from: http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf [Accessed 20 April 2011]

Nazemi, N. (2011) Safe Harbour for Anonymity Networks amid a Cyber-Democratic Storm: Lessons from the 2009 Iranian Uprising. *North-Western University Law Review*, **106**

NBC (2013) Iran's Approaching Vote Brings Receding Web Access. *NBCNews.com*. Published 27 May 2013. Available from: <http://www.nbcnews.com/technology/irans-approaching-vote-brings-receding-web-access-6C10088197> [Accessed 20 September 2013]

Near East Observatory (2013) 14-year-old Blogger Arrested in Iran. Published 1 January 2013. Available from: <http://neobservatory.org/censorship/14-year-old-blogger-arrested-in-iran> [Accessed 19 September 2013]

Neff, G., Jordan, T., McVeigh-Schultz, J. and Gillespie, T. (2012) Affordances, Technical Agency and the Politics of Technologies of Cultural Production. *Journal of Broadcasting and Electronic Media*. **56**(2): 299–313

Negroponte, N., Harrington, R., McKay, S.R. and Christian, W. (1997) Being Digital. *Computers in Physics*. **11**(3): 261–62

Neriya-Ben Shahar, R. and Lev-On, A. (2011) Gender, Religion, and New Media: Attitudes and Behaviours Related to the Internet among Ultra-Orthodox Women Employed in Computerised Environments. *International Journal of Communication*. 5(2011): 875c95

Net Index (2013) Household Download Index 2013. Published 1 October 2013. Available from: <http://www.netindex.com/download/allcountries> [Accessed 4 October 2013]

New America Media (2011) Brain Drain: Destroying Iran One University Graduate at a Time. Published 23 October 2011. San Francisco, CA, USA. Available from: <http://newamericamedia.org/2011/10/brain-drain-destroying-iran-one-university-graduate-at-a-time.php> [Accessed 4 December 2013]

New York Times (1991) In US Technology, a Gap Between Arms and VCR's. *The New York Times Company*. Published 4 March 1991. Available from: <http://www.nytimes.com/1991/03/04/business/in-us-technology-a-gap-between-arms-and-vcr-s.html?pagewanted=all&src=pm> [Accessed 12 October 2013]

Newman, N. (2009) The Rise of Social Media and Its Impact on Mainstream Journalism. *Reuters Institute for the Study of Journalism*. Oxford University. Oxford, UK. Available from: https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/The_rise_of_social_media_and_its_impact_on_mainstream_journalism.pdf [Accessed 20 September 2013]

NIAC (2010) H.R.4303—The Stand With The Iranian People Act (SWIPA). *National Iranian-American Council*. Washington DC, USA. Available from: http://www.niacouncil.org/images/PDF_files/swipa%20one%20page.pdf [Accessed 1 October 2013]

Niklasson, L. (2013) Competing Narratives on the European Social Model: The Birth of a Rhetorical Alliance. *European Integration in Swedish Economic Research: Discussion Paper*. Grand Hotel, Mölle, Sweden

Niosi, J., Saviotti, P., Bellon, B. and Crow, M. (1993) National Systems of Innovation: In Search of a Workable Concept. *Technology in Society*. 15(2): 207–27

Noble, P. (2008) Six Big Ideas: ICT as a Vital Tool for Reform. In: S. Odugbemi and T. Jacobson (Eds.) *Governance Reform under Real-world Conditions: Citizens, Stakeholders and Voice*. The International Bank for Reconstruction and Development / The World Bank. Washington DC, USA

Nokia-Siemens Networks (2009) Provision of Lawful Intercept capability in Iran. Espoo, Finland. Available from: http://www.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_2009_06_22_enProvision-of-Lawful-Intercept-capability-in-Iran.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010a) Response to lawsuit filed by Isa and Mehdi Saharkhiz against Nokia Siemens Networks. Espoo, Finland. Available from: http://www.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_2010_08_20_en_Saharkhiz_response_0.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010b) Clarification on Nokia Siemens Networks' Business in Iran. Espoo, Finland. Available from:
http://www.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_2010_09_28_en_Clarification-on-NSN-business-in-Iran.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010c) Saharkhiz Lawsuit Voluntarily Withdrawn by Plaintiffs. Espoo, Finland. Available from:
http://www.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_2010_11_11_en_Saharkhiz_withdrawal_1.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010d) Response to UANI Campaign. Espoo, Finland. Available from:
http://ru.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_2010-10-03_en_NSN-reply-to-UANI-letter.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010e) Statement from Barry French Executive Board Member and Head of Marketing and Corporate Affairs Nokia Siemens Networks. Espoo, Finland. Available from:
http://www.nokiasiemensnetworks.com/sites/default/files/document/NokiaSiemensNetworks_201006_02_en_Iran_Statement.pdf [Accessed 20 April 2011]

Nokia-Siemens Networks (2010f) "This sure doesn't look like Kansas, Toto": Ethics vs. an Unrelenting World. Published July 2010. Espoo, Finland. Available from:
<http://www.scu.edu/ethics/practicing/focusareas/business/Rob%20Weisberg--Final.pdf> [Accessed 1 October 2013]

NPR (2011) Iran Charges Student Who Was in the US. Published 7 October 2011. Available from: <http://www.npr.org/2011/10/07/141090966/iran-charges-student-who-was-in-the-u-s> [Accessed 2 November 2013]

Nye, J.S. (2010) Cyber Power. *Belfer Centre for Science and International Affairs at Harvard Kennedy School*. Harvard University. Cambridge, MA, USA. Available from:
<http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf> [Accessed 20 April 2011]

O'Lear, S. (2015) Climate Science and Slow Violence: A View from Political Geography and STS on Mobilising Techno-Scientific Ontologies of Climate Change. *Political Geography*. Amsterdam, Netherlands: Elsevier Ltd.

O'Shaughnessy, S. and Krogman, N.T. (2012) A Revolution Reconsidered? Examining the Practice of Qualitative Research in Feminist Scholarship. *Signs*. **37**(2): 493–520

Olsen, W. (2004) Triangulation in Social Research: Qualitative and Quantitative Methods can Really be Mixed. *Developments in Sociology*. **20**: 103–18

OpenNet Initiative (2005) Internet Filtering in Iran. Available from:
http://opennet.net/sites/opennet.net/files/ONI_Country_Study_Iran.pdf [Accessed 9 August 2011]

OpenNet Initiative (2011a) Iran Ranked as World's Worst Internet Oppressor. Published 28 April 2011. Available from: <https://opennet.net/blog/2011/04/iran-ranked-world's-worst-internet-oppressor> [Accessed 10 December 2013]

OpenNet Initiative (2011b) West Censoring East: The Use of Western Technologies by Middle East Censors. Available from: http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf [Accessed 20 April 2011]

OpenNet Initiative (2013) After the Green Movement: Internet Controls in Iran, 2009–2012. Published February 2013. Available from: <https://opennet.net/sites/opennet.net/files/iranreport.pdf> [Accessed 1 October 2013]

Oudshoorn, N., Rommes, E. and Stienstra, M. (2004) Configuring the User as Everybody: Gender and Design Cultures in Information and Communication Technologies. *Science, Technology and Human Values*. **29**(1): 30–63

Outsourcing Centre (2005) Ukraine: Will the Orange Revolution Boost the IT Outsourcing Industry? *Outsourcing Centre*. Published 1 October 2005. Available from: <http://www.outsourcing-center.com/2005-10-ukraine-will-the-orange-revolution-boost-the-it-outsourcing-industry-article-37674.html> [Accessed 15 October 2013]

Padoch, C. and Sunderland, T.C.H. (2014) Managing Landscapes for Greater Food Security and Improved Livelihoods. *Unasylva*: **64**(241). Centre for International Forestry Research (CIFOR). Bogor, Indonesia

Pain, R. (2003) Social Geography: On Action-Orientated Research. *Progress in Human Geography*. **27**(5): 649–658

Palczewski, C.H. (2001) Cyber-Movements, New Social Movements, and Counter-Publics. *Counter-Publics and the State*. Pages: 161–86

Paley, J. and Lilford, R.J. (2011) Qualitative Methods: An Alternative View. *BMJ*. **342**(7804): 956–958

Papic, M. and Noonan, S. (2011) Social Media as a Tool for Protest. *Stratfor Global Intelligence*: **3**

Parameswaran, A. and Polyzotis, N. (2011) Answering Queries Using Humans, Algorithms and Databases. In: *Fifth Biennial Conference on Innovative Data Systems Research*. Published January 2011. Monterey, CA, USA. pp. 160–66

Paris, J. (2011) Prospects for Iran. *Legatum Institute*. Paper Commissioned in January 2011 for the Legatum Institute's *The Future of Iran* Workshop on Economic Reform. London, UK. Available from: <http://www.li.com/docs/publications/2011-publication-prospects-for-iran.pdf> [Accessed 9 June 2012]

Pars Times (2000) Why Iranian Students Going Abroad for Higher Education Refuse to Return Home? Published January 2000. **7**: 20–3. [online]. Available from: http://www.parstimes.com/education/students_abroad.html [Accessed 27 September 2015]

- Patel, P. and Pavitt, K. (1998) National Systems of Innovation under Strain: The Internationalisation of Corporate R&D. *Science Policy Research Unit (SPRU) at University of Sussex*. Sussex, UK. Published May 1998. Available from: <http://www.druid.dk/conferences/summer1999/conf-papers/Pavitt.pdf> [Accessed 18 September 2011]
- Patterson, J.P. and Smith M.N. (2005) Developing A Reliable Methodology for Assessing the Computer Network Operations Threat of Iran. *Naval Postgraduate School*. Monterey, CA, USA. Available from: <http://www.fas.org/irp/eprint/cno-iran.pdf> [Accessed 27 July 2011]
- Pettersson, R. (1982) Cultural Differences in the Perception of Image and Colour in Pictures. *Educational Technology Research and Development*. **30**(1): 43–53
- Petray, T.L. (2010) Actions, Reactions and Interactions: The Townsville Aboriginal Movement and the Australian State. *Doctoral Dissertation*. James Cook University. Queensland, Australia
- Paulsen, F. (2007) The Impact of EU's Policies on Democratisation in Sub-Sahara Africa. University of Twente. Enschede, Netherlands. Published 22 February 2007. Available from: http://essay.utwente.nl/706/1/scriptie_Paulsen.pdf [Accessed 17 October 2013]
- PBS (2008) Activists Face Obstacles Online in Winning Women's Rights in Iran. *Public Broadcasting Service*. Toronto, Canada. Published 16 September 2008. Available from: <http://www.pbs.org/mediashift/2008/09/activists-face-obstacles-online-in-winning-womens-rights-in-iran260> [Accessed 11 September 2013]
- PBS (2009) Geeks Around the Globe Rally to Help Iranians Online. *Public Broadcasting Service*. Toronto, Canada. Published 08 July 2009. Available from: <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2009/07/geeks-around-the-globe-rally-to-help-iranians-online.html> [Accessed 11 September 2013]
- Phillips, M. (2014) Re-Writing Corporate Environmentalism: Ecofeminism, Corporeality and the Language of Feeling. *Gender, Work and Organisation*. **21**(5): 443–58
- Pickard, V.W. (2008) Co-Optation and Cooperation: Institutional Exemplars of Democratic Internet Technology. *New Media and Society*. **10**(4): 625–45
- Pillar Fourth Committee (2011) Launching Distribution of Free VPNs among Iranian Users. Published 21 August 2011. Available from: http://hraicp.org/index.php?option=com_content&view=article&id=67:000&catid=1:000&Itemid=5 [Accessed 10 September 2013]
- Pinch, T. (2008) Technology and Institutions: Living in a Material World. *Theory and Society*. **37**(5): 461–83
- Pinch, T. and Bijker, W.E. (1986) Science, Relativism and the New Sociology of Technology: Reply to Russell. *Social Studies of Science*. **16**: 347–60. London, UK: SAGE Publications Ltd.

- Pinto, H. and Santos-Pereira, T. (2013) Efficiency of Innovation Systems in Europe: An Institutional Approach to the Diversity of National Profiles. *European Planning Studies*. **21**(6): 755–779
- Polese, A. (2008) Russia, the US, the Others and the 101 Things to Do to Win a (Colour) Revolution: Reflections on Georgia and Ukraine. *Paper presented at the CEELBAS Workshop "Colour Revolutions in Eurasia" at King's College, University of Cambridge on 30 April 2008*. Cambridge, UK
- Polyuha, M. (2005) Ukrainian Internet Identity. *Western Journal of Graduate Research*. **12**(1): 82–91. University of Western Ontario. London, ON, Canada
- Porat, Y. (2012) Iranians Have Democratic Values. *The Wall Street Journal*. Published 13 May 2012. [online]. Available from: <http://www.wsj.com/articles/SB10001424052702304363104577392050519982974> [Accessed 01 July 2016]
- Porch, D. (2013) Counterinsurgency: Exposing the Myths of the New Way of War. Cambridge, UK: *Cambridge University Press*
- Posch, W. (2010) A Last Chance for Iran's Reformists? The Green Struggle Reconsidered. *Working Paper based on a presentation delivered on 17 March 2010 at the European Parliament*. Middle East and Africa Division, German Institute for International and Security Affairs. Berlin, Germany
- Posner, M.V. (1961) International Trade and Technical Change. *Oxford Economic Papers*. **13**(3): 323–41
- Pritchard, A. (2014) Many VPNs and Psiphon are Currently Blocked in Iran. *Psiphon Inc.* Published 25 February 2014. Toronto, Canada. Available from: <https://mailman.stanford.edu/pipermail/liberationtech/2014-February/013015.html> [Accessed 02 September 2014]
- Psaki, J. (2013) United States Takes Action to Facilitate Communications by the Iranian People and Targets Iranian Government Censorship. *US Department of State*. Published 30 May 2013. Washington DC, USA. Available from: <http://www.state.gov/r/pa/prs/ps/2013/05/210102.htm> [Accessed 11 September 2013]
- Puleo, A.H. (2012) From Cyborgs to Organic Model and Back: Old and New Paradoxes of Gender and Hybridity. *Comparative Critical Studies*. **9**(3): 349–64
- Qi, C. (2011) A Study on a New Framework of the National Innovation System. In: *Business Management and Electronic Information International Conference*. Published May 2011. **1**: 228–231
- Qiu, J.L., Castells, M. and Cartier, C. (2009) Working-Class Network Society: Communication Technology and the Information Have-Less in Urban China. Cambridge, MA, USA: *MIT Press*

Radio Free Europe/Radio Liberty (2011) 'Anonymous' Hackers Help Iranian Activists Fight The Regime. Published 18 February 2011. Prague, Czech Republic. Available from: http://www.rferl.org/content/iran_hackers_anonymous_cyberarmy_opposition_internet/2313350.html [Accessed 13 September 2013]

Rangelov, I. (2013) Democracy or Stability? European Approaches to Justice in Peace and Transitional Processes. *Global Policy*. Hoboken, New Jersey: Wiley-Blackwell

Reason, P. and Bradbury, H. (2013) The SAGE Handbook of Action Research: Participative Inquiry and Practice. Thousand Oaks, CA, USA: *SAGE Publications Ltd*.

Reddy, M. (2013) Mobile Health Applications: Designing with the User in Mind. *Association for Computing Machinery*. Published 5 February 2013. Available from: http://www.computingreviews.com/hottopic/hottopic_essay_11.cfm [Accessed 17 December 2013]

Reporters Without Borders (2012) Cyber-Censorship in 2012: Iran. Paris, France. Available from: <http://surveillance.rsf.org/en/iran> [Accessed 1 October 2013]

Reuters (2012) Special Report: Chinese Firm Helps Iran Spy on Citizens. *Thomson Reuters*. Available from: <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322> [Accessed 12 September 2013]

Rezazadeh-Mehrizi, M.H. and Pakneiat, M. (2008) Comparative Analysis of Sectorial Innovation System and Diamond Model: The Case of Telecom Sector of Iran. *Journal of Technology Management and Innovation*. **3**(3): 78–90

Ria Novosti (2010) EU Challenges Iranian Satellite Jamming. Moscow, Russia. Available from: <http://en.rian.ru/world/20100322/158276728.html> [Accessed 11 September 2013]

Rizk, N.J. (2003) Productive Face-to-Face Interview. *Computer Based Learning in Science*. 972–86

Roettgers, J. (2009) LimeWire Helps Circumvent Iranian Internet Censorship. *P2P-Blog.com*. Published 28 June 2009. Available from: <http://www.p2p-blog.com/item-1097.html> [Accessed 11 September 2013]

Rogers, E.M. (1983) Diffusion of Innovations. Third Edition. New York, USA: *The Free Press, Simon and Schuster, Inc*.

Roos Online (2010) 1388: Year of Militarisation of Economy. Published 22 March 2010. Tehran, Iran. Available from: <http://www.roosonline.com/english/news3/newsitem/article/1388-year-of-militarization-of-economy.html> [Accessed 11 September 2013]

Rouse, W.B. (2003) Engineering Complex Systems: Implications for Research in Systems Engineering. *IEEE Transactions on Systems, Man and Cybernetics – Part C*. **33**(2): 154–56

Rowbotham, S. (2013) Women in Movement: Feminism and Social Action. London, UK: *Routledge*

- Royal Danish Defence College (2013) Brief: Security Sector Reform in an Unstable, Fragile State (II/III). *Institute for Strategy*. Published January 2013. Copenhagen, Denmark. Available from: <http://forsvaret.dk/FAK/Publikationer/Briefs/Documents/Security%20Sector%20Reform%20in%20an%20Unstable,%20Fragile%20State.pdf> [Accessed 1 October 2013]
- Russell, B. (1953) *The Impact of Science on Society*. New York, USA: AMS Press
- Ruttan, V.W. (1997) Induced Innovation, Evolutionary Theory and Path Dependence: Sources of Technical Change. *The Economic Journal*. **107**(444): 1520–29
- Sabeti, A. (2011) New Light Shed on the Iranian Cyber Army. *Iran Media Research*. Available from: <http://iranmediaresearch.org/en/blog/13/11/03/24/388> [Accessed 14 July 2011]
- Salami, R. (2008) Reshaping and Reforming National Innovation System toward Knowledge Based Economy: Some Particular Lessons from Iran's Experience. *Oxford Department of International Development at Oxford University*. Oxford, UK. Available from: <http://www3.geh.ox.ac.uk/slptmd/Salami.pdf> [Accessed 25 August 2011]
- Salnykova, A. (2006) *The Orange Revolution: A Case Study of Democratic Transition in Ukraine*. Simon Fraser University. Published Spring 2006. Burnaby, BC, Canada. Available from: <http://summit.sfu.ca/system/files/iritems1/2456/etd2260.pdf> [Accessed 15 October 2013]
- Sawyer, S. and Rosenbaum, H. (2000) Social Informatics in the Information Sciences: Current Activities and Emerging Directions. *Informing Science*. **3**(2): p. 89
- Science Metrix (2010) Geopolitical Shifts in Knowledge Creation Since 1980. Published February 2010. Available from: <http://www.science-metrix.com/30years-Paper.pdf> [Accessed 1 October 2013]
- Sclove, R. (1997) Research by the People: Building a Worldwide Community Research Network. In: T. Schroyer (Ed.) *A World that Works: Building Blocks for a Just and Sustainable Society*. New York, NY, USA: Bootstrap Press
- Scott, A. (2012) From First Tweet to Final Collapse: The Dimensions of Social Media in Regime Collapse. *Paper Prepared for the International Studies Association Annual Convention*. Published April 2012. San Diego, CA, USA
- Seale, C. (1999) Quality in Qualitative Research. *Qualitative Inquiry*. **5**(4): 465–78
- Searls, D. and Sifry, D. (2003) Building with Blogs. *Linux Journal*. **4**(107)
- Seattle Times (2009) Pro-Shah Iranians Call for Regime Change. *The Seattle Times Company*. Published 16 June 2009. Available from: http://seattletimes.com/html/nationworld/2009331739_apusiranelectionus.html [Accessed 10 December 2013]

Secor, A.J. and O'Loughlin, J. (2005) Social and Political Trust in Istanbul and Moscow: A Comparative Analysis of Individual and Neighbourhood Effects. *Royal Geographical Society (with The Institute of British Geographers)*. Published 24 March 2005. Available from: http://www.colorado.edu/ibs/pec/johnno/pub/istanbul_moscow.pdf [Accessed 17 October 2013]

Seib, P. (2012) *Real-Time Diplomacy: Politics and Power in the Social Media Era*. Basingstoke, UK: *Palgrave Macmillan*

Seidman, I. (2013) *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. *Columbia University*. New York, NY, USA: *Teachers College Press*

Selwyn, N. (2003) Apart From Technology: Understanding People's Non-Use of Information and Communication Technologies in Everyday Life. *Technology in Society*. **25**(1): 99–116

Selwyn, N. (2004) Reconsidering Political and Popular Understandings of the Digital Divide. *New Media and Society*. **6**(3): 341–62

Shahab, C.J. and Mousoli, R. (2010) Traffic Analysis, Anonymity, Freedom and Digital Cat and Mouse in Cyberspace: A Case Study of China vs. Iran. Available from: <http://payvand.com/news/10/sep/Traffic-Analysis--C.Shahab--R.Mousoli.pdf> [Accessed 20 April 2011]

Shahrzad News (2012) Equipping Governmental Institutions with Proxy Software and VPNs following Gmail Blockage! Published 29 September 2012. Available from: <http://www.1001nights.org/index.php?page=1andnewsItemId=7876andcontentFilterLocation=iran> [Accessed 10 September 2013]

Shapiro, E. (2010) *Gender Circuits: Bodies and Identities in a Technological Age*. London, UK: *Routledge*

Shapiro, M.A., So, M. and Woo-Park, H. (2010) Quantifying the National Innovation System: Inter-Regional Collaboration Networks in South Korea. *Technology Analysis and Strategic Management*. **22**(7): 845–857

Shipman, M.D. (2014) *The Limitations of Social Research*. London, UK: *Routledge*

Shyyan, V. (2008) *Democracy in Ukraine After the Orange Revolution: Youth Activists' Insights on Past Events, Present Efficacy and Future Prospects*. University of Minnesota. Minneapolis, MN, USA. Available from: http://conservancy.umn.edu/bitstream/91521/1/Shyyan_Vitaliy%20Sept%202008.pdf [Accessed 6 August 2012]

Sigurdson, J. (2004) Regional Innovation Systems in China. *European Institute of Japanese Studies working paper 195*. Stockholm, Sweden

SIPRI (2013) SIPRI Data on Military Expenditure in 171 Countries. *Stockholm International Peace Research Institute*. Stockholm, Sweden. Available from: <http://portal.sipri.org/publications/pages/expenditures/download-database> [Accessed 18 December 2013]

Smith, A. (1776) *An Enquiry into the Nature and Causes of the Wealth of Nations*. 5th Edition, Reprinted in 1937. New York, USA: *Random House*

Smith, A. (2005) Environmental Movements and Innovation: From Alternative Technology to Hollow Technology. *Human Ecology Review*: **12**(2)

Smith, N.J. and Lee, D. (2015) What's Queer about Political Science? *The British Journal of Politics and International Relations*. **17**(1): 49–63

Smith, K., Paranjape, R. and Benedicenti, L. (2001) Agent Behaviour and Agent Models in Unregulated Markets. *ACM SIGAPP Applied Computing Review*: **9**(3)

Sofka, W. (2005) Global Idea Sourcing: An Empirical Investigation into the Mechanisms Behind the Usage of Foreign Business Sources for Innovation. *Centre for European Economic Research*. Discussion Paper No. 05-53. Published 19 July 2005. Mannheim, Germany. Available from: <ftp://ftp.zew.de/pub/zew-docs/dp/dp0553.pdf> [Accessed 18 October 2013]

Sohrabi-Haghighat, H. and Mansouri, S. (2010) 'Where Is My Vote?' ICT Politics in the Aftermath of Iran's Presidential Election. *International Journal of Emerging Technologies and Society*. **8**(1): 24–41

Som, C., Hilty, L.M. and Ruddy, T.F. (2004) The Precautionary Principle in the Information Society. *Human and Ecological Risk Assessment*. **10**(5): 787–799

Soofi, A.S., Ghazinoory, S. and Farnoodi, S. (2013) The National Innovation System of Iran: A Functional and Institutional Analysis. In: A.S. Soofi and S. Ghazinoory (Eds.) *Science and Innovations in Iran*. pp. 57–86. New York, NY, USA: Palgrave Macmillan

Souitaris, V. (1999) Research on the Determinants of Technological Innovation: A Contingency Approach. *International Journal of Innovation Management*. **3**(3): 287–305

Spencer, L. and Ritchie, J. (2012) In Pursuit of Quality. In: D. Harper and A.R. Thompson (Eds.) *Qualitative Research Methods in Mental Health and Psychotherapy: A Guide for Students and Practitioners*. John Wiley and Sons, Ltd: 225–42. Chichester, UK

Spiegel Online (2003) Weapons of Mass Destruction: Iranian Exiles Expose Tehran Secret Bio-Weapons Research. Published 16 May 2003. Hamburg, Germany. Available from: <http://www.spiegel.de/politik/ausland/massenvernichtungswaffen-exil-iraner-werfen-teheran-heimliche-biowaffenforschung-vor-a-248893.html> [Accessed 20 April 2011]

Spy Blog (2009) Satellite Jammers in Iran? Published 20 July 2009. Available from: <http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/07/20/satellite-jammers-in-iran.html> [Accessed 27 August 2011]

- Starosta De Waldemar, F. (2010) New Products and Corruption: Evidence from Indian Firms. *Centre d'Economie de la Sorbonne, Université Paris 1 Panthéon Sorbonne*. Paris, France. Published February 2010. Available from: <http://www.csae.ox.ac.uk/conferences/2011-EDiA/papers/035-Waldemar.pdf> [Accessed 1 October 2013]
- Stein, J.A. (2002) Science, Technology and European Foreign Policy: European Integration, Global Interaction. *Science and Public Policy*. **29**(6): 463–77
- Stepanova, E. (2011) The Role of Information Communication Technologies in the Arab Spring. *Ponars Eurasia* (15): 1–6
- Stohl, M. (2007) Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games? *Springer Science + Business Media*. Available from: http://ceps.anu.edu.au/publications/pdfs/stohl_pubs/stohl_cyber_terrorism_a_clear_and_present_danger.pdf [Accessed 20 April 2011]
- Strinde, G. (2011) Cyber Warfare: Connecting Classical Security Theory to a New Security Domain. Department of Political Science, Peace and Conflict Studies, Lund University. Published Spring 2011. Lund, Sweden. Available from: <http://lup.lub.lu.se/luur/download?func=downloadFile&recordId=1970395&fileId=1970396> [Accessed 02 September 2014]
- Sturges, R.P. (2010) The Mobile Phone And Access to Information in the Developing World: Identifying the Ethical Dimensions. Available from: <http://moriarty.tech.dmu.ac.uk:8080/pebble/repository/files/publications/R%20P%20Sturges%20ETICA%20Paper.pdf> [Accessed 20 April 2011]
- Sun, S.L., Chen, H. and Pleggenkuhle-Miles, E.G. (2010) Moving Upward in Global Value Chains: The Innovations of Mobile Phone Developers in China. *Chinese Management Studies* **4**(4): 305–21. Bingley, UK: *Emerald Group Publishing*
- Sun, Y. (2002) Sources of Innovation in China's Manufacturing Sector: Imported or Developed In-House? *Environment and Planning*. **34**(6): 1059–72
- Sun, Y. and Du, D. (2010) Determinants of Industrial Innovation in China: Evidence from Its Recent Economic Census. *Technovation*. **30**(9): 540–50
- Sun, Y. and Liu, F. (2010) A Regional Perspective on the Structural Transformation of China's National Innovation System Since 1999. *Technological Forecasting and Social Change*. **77**(8): 1311–21
- Suttmeier, R.P., Cao, C. and Simon, D.F. (2006) Knowledge Innovation and the Chinese Academy of Sciences. *American Association for the Advancement of Science*. Published April 2006
- Suzuki, D. and Mayorga, E. (2014) Scholar-Activism: A Twice Told Tale. *Multicultural Perspectives*. **16**(1): 16–20

- Swift, C. (2003) Access Denied: We Have Photographic Evidence of Iranian Censorship of the Net. *The Daily Summit*. Published 11 December 2003. Available from: http://www.dailysummit.net/english/archives/2003/12/11/access_denied_.asp [Accessed 17 April 2011]
- Tabnak (2009) Official Disclosure of the Cyber Crime Law. Published 29 December 2009. Tehran, Iran. Available from: <http://www.tabnak.ir/fa/pages/?cid=79090> [Accessed 10 September 2013]
- Taheri, A. (2007) Who Are Iran's Revolutionary Guards? *The Wall Street Journal*. Published 15 November 2007. [online]. Available from: <http://www.wsj.com/articles/SB119509278241693687> [Accessed 28 September 2015]
- Tahmasebi-Birgani, V. (2010) Green Women of Iran: The Role of the Women's Movement during and After Iran's Presidential Election of 2009. *Constellations*. **17**(1): 78–86
- Tan, X. (2010) Clean Technology R&D and Innovation in Emerging Countries: Experience from China. *Energy Policy*. **38**(6): 2916–26
- Tavokin, E.P. (2011) Mass Communication in the Modern World. *Herald of the Russian Academy of Sciences*. **81**(6): 608–13
- Tech Eye Network (2013) Iran Wastes Time Blocking VPNs. *JAM IT Media Ltd*. Published 12 March 2013. Available from: <http://news.techeye.net/internet/iran-wastes-time-blocking-vpns> [Accessed 16 September 2013]
- Tedre, M., Sutinen, E., Kähkönen, E. and Kommers, P. (2006) Ethno-Computing: ICT in Cultural and Social Context. *Communications of the ACM*. **49**(1): 126–130
- Tehran Times (2010) Iran Advances 41 Places in Industrial Production. *Tehran Times*. Published 28 February 2010. Tehran, Iran. Available from: http://web.archive.org/web/20120820025409/http://old.tehrantimes.com/index_View.asp?code=215089 [Accessed 2 November 2013]
- Teixeira, E.D.O. and Werther W.B. (2013) Resilience: Continuous Renewal of Competitive Advantages. *Business Horizons*. **56**(3): 333–42
- TeleGeography (2009) Etemad-e-Mobin Score TCI coup. *PriMetrica, Inc*. Published 28 September 2009. Available from: <http://www.telegeography.com/products/commsupdate/articles/2009/09/28/etemad-e-mobin-score-tci-coup> [Accessed 19 September 2013]
- Telegraph (2013) Iranian Ministers Open Pages on Banned Facebook. *Telegraph Media Group Ltd*. Published 9 September 2013. Available from: <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10296294/Iranian-ministers-open-pages-on-banned-Facebook.html> [Accessed 1 October 2013]
- Tenhunen, S. (2008) Mobile Technology in the Village: ICTs, Culture, and Social Logistics in India. *Journal of the Royal Anthropological Institute*. **14**(3): 515–34

Thomas, M. and Mohaisen, A. (2014) Measuring the Leakage of Onion at the Root: A Measurement of TOR. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. Published November 2014: pp. 173–80

Thornham, H. and McFarlane, A. (2014) Claiming Content and Constructing Users: User-Generated Content and BBC Blast. In: M.J. Kehily, D. Buckingham and S. Bragg (Eds.) *Youth Cultures in the Age of Global Media*. pp. 86–201. London, UK: Palgrave Macmillan

Time (2009) Iran Protests: Twitter, the Medium of the Movement. *Time Inc.* Published 17 June 2009. Available from: <http://content.time.com/time/world/article/0,8599,1905125,00.html> [Accessed 1 October 2013]

Tohidi, N. (1991) Gender and Islamic Fundamentalism: Feminist Politics in Iran. In: C.T. Mohanty and A. Russo (Eds.) *Third World Women and the Politics of Feminism*. pp. 251–70. Bloomington, IN, USA: Indiana University Press

Toronto Star (2013) Iranian-Canadians Enable Internet Access for Countrymen Back Home. *Toronto Star Newspapers Ltd.* Published 17 May 2013. Toronto, Canada. Available from: http://www.thestar.com/news/immigration/2013/05/17/iraniancanadians_enable_internet_access_for_countrymen_back_home.html [Accessed 12 September 2013]

Torrent Freak (2013) AT&T Invents New Technology to Detect and Ban File-Sharing. Published 15 December 2013. Available from: <http://torrentfreak.com/att-invents-new-technology-to-detect-and-ban-filesharing-131214> [Accessed 18 December 2013]

Tracy, S.J. (2010) Qualitative Quality: Eight Big-Tent Criteria for Excellent Qualitative Research. *Qualitative Inquiry*. **16**(10): 837–51

Transparency International (2011) National Integrity System Assessment: Ukraine. Published 9 May 2011. Berlin, Germany. Available from: http://files.transparency.org/content/download/82/327/file/2011_NISUkraine_EN.pdf [Accessed 12 October 2013]

Transparency International (2012) Corruption Perceptions Index 2012. Berlin, Germany. Available from: http://files.transparency.org/content/download/537/2229/file/2012_CPI_brochure_EN.pdf [Accessed 1 October 2013]

Tucker, J.B. (2012) *Innovation, Dual-Use and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. MA, USA: MIT Press

Umbrecht, A. and Esser, F. (2013) Changing Political News? Long-Term Trends in American, British, French, Italian, German and Swiss Print Media Reporting. *Political Journalism in Transition: Western Europe in a Comparative Perspective*. **195**

United Nations (2005) Science, Technology and Innovation Policy Review: The Islamic Republic of Iran. *United Nations' Conference on Trade and Development*. NY, USA. Available from: http://www.unctad.org/en/docs/iteipc20057_en.pdf [Accessed 25 August 2011]

United Nations Development Programme (2011) Human Development Report—Sustainability and Equity: A Better Future for All. *United Nations*. NY, USA. Available from: http://hdr.undp.org/en/media/HDR_2011_EN_Complete.pdf [Accessed 31 August 2013]

United States House of Representatives (2012) Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. *A Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence*. Published 8 October 2012. Available from: [http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf) [Accessed 1 October 2013]

United States Institute of Peace (2013) Report: Is Iran a Cyber Power? *United States Institute of Peace*. Published 29 July 2013. Washington DC, USA. Available from: <http://iranprimer.usip.org/blog/2013/jul/29/report-iran-cyber-power> [Accessed 10 December 2013]

United States Treasury Department (2012) Fact Sheet: New Executive Order Targeting Human Rights Abuses Via Information Technology. *Office of Public Affairs*. Published 23 April 2012. Available from: <http://iran.usembassy.gov/treasuryfactsheet.html> [Accessed 11 September 2013]

Uskowi, N. (2013) Rouhani Wins Big Among Expats. *Uskowi on Iran*. Published 6 July 2013. Available from: <http://www.uskowioniran.com/2013/07/rouhani-wins-big-among-expats.html> [Accessed 2 October 2013]

Vakil, S. (2011) Women and Politics in the Islamic Republic of Iran: Action and Reaction. New York, USA: *The Continuum International Publishing Group*

Valeriano, B. and Maness, R. (2012) Persistent Enemies and Cyber War: Rivalry Relations in an Age of Information Warfare. In: D.S. Reveron (Ed.) *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. Washington DC, USA: Georgetown University Press

Valkenburg, G. (2012) Sustainable Technological Citizenship. *European Journal of Social Theory*. **15**(4): 471–87

Valovirta, V. (2012) Towards a Management Framework for Public Procurement of Innovation. In Conference: *Demand, Innovation and Policy*. Manchester Institute of Innovation Research. Published March 2012. Manchester, UK. pp. 22–3

Van Berkel, R., Sager, F. and Ehrler, F. (2012) The Diversity of Activation Markets in Europe. *International Journal of Sociology and Social Policy*. **32**(5/6): 273–85

Van De Donk, W., Loader, B.D., Nixon, P.G. and Rucht, D. (2004) Cyber-Protest: New Media, Citizens and Social Movements. London, UK: *Routledge*

Van Laer, J. and Van Aelst, P. (2009) Cyber-Protest and Civil Society: The Internet and Action Repertoires in Social Movements. *Handbook on Internet Crime*: 230–254

- Van Lobberegt, M. (2012) Geographic Distance and Differences in Corporate Governance Code Adoption: An Institutional Approach. University of Amsterdam. Published 20 July 2012. Amsterdam, UK. Available from: <http://dare.uva.nl/document/478185> [Accessed 18 October 2013]
- Varisco, A.E. (2014) The Influence of Research and Local Knowledge on British-Led Security Sector Reform Policy in Sierra Leone. *Conflict, Security and Development*. **14**(1): 89–123
- Vaughn, Z.C. (2005) Hacktivism: Civil Rights Activism in the Digital Age. University of Texas at Tyler. Tyler, TX, USA. Available from: http://zaxxon.net/eportfolio/projects/philo/HacktivismResearch_ZV.pdf [Accessed 20 April 2011]
- Venger, O. (2006) Globalisation: Aid or Constraint to the Democratic Function of the Media? Revolutions in Serbia and Ukraine. *Conference Paper on Communication Methods of Velvet Revolutions*. Published 18 September 2006. Publication ID: 103-430-079
- Voelker, J. (2005) Conference Report: Changing Patterns of Security in the Middle East and Central Asia. *A Workshop Co-Hosted on 18 May 2005 by the Department of National Security Affairs at the Naval Postgraduate School and the Centre for Strategic Studies at the CNA Corporation*. Alexandria, VA, USA. Available from: http://www.nps.edu/ccf/conferences/recent/may05changingpatterns_rpt.pdf [Accessed 1 October 2013]
- Von Hippel, E. (1976) The Dominant Role of Users in the Scientific Instrument Innovation Process. *Research Policy*. **5**(3): 212–39
- Von Neumann, J. and Morgenstern, O. (1944) Theory of Games and Economic Behaviour. Princeton, NJ, USA: *Princeton University Press*
- Wade, R.H. (2011) Emerging World Order? From Multi-Polarity to Multilateralism in the G20, the World Bank and the IMF. *Politics and Society*. **39**(3): 347–78
- Wajcman, J. (2007) From Women and Technology to Gendered Techno-Science. *Information, Community and Society*. **10**(3): 287–98
- Wajcman, J. (2008) Life in the Fast Lane? Towards a Sociology of Technology and Time. *The British Journal of Sociology*. **59**(1): 59–77
- Wajcman, J. (2009) Feminist Theories of Technology. *Cambridge Journal of Economics*. Oxford, UK: *Oxford University Press*
- Wajcman, J. (2013) Techno-Feminism. Hoboken, NJ, USA: *John Wiley and Sons*
- Walker, D.H. (1970) Political Ideology and Personality Correlates of College Students and their Response to a Request for Helping Behaviour from a Politically Biased Recruiter. *Master's Dissertation (Thesis 2057)*. University of Massachusetts Amherst. MA, USA

Wall Street Journal (2009) Thousands Flee Iran as Noose Tightens. *Dow Jones and Company, Inc.* Published 11 December 2009. Available from: http://online.wsj.com/article/SB126049484505086861.html?mod=rss_Today's_Most_Popular [Accessed 5 October 2013]

Wall Street Journal (2011a) Chinese Tech Giant Aids Iran. *Dow Jones and Company, Inc.* Published 27 October 2011. Available from: <http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html> [Accessed 12 September 2013]

Wall Street Journal (2011b) Huawei to Scale Back Business in Iran. *Dow Jones and Company, Inc.* Published 10 December 2011. Available from: <http://online.wsj.com/article/SB10001424052970204319004577088001900708704.html> [Accessed 12 September 2013]

Wall Street Journal (2011c) Nokia-Siemens Venture to Reduce Its Business in Iran. *Dow Jones and Company, Inc.* Published 14 December 2011. Available from: <http://online.wsj.com/article/SB10001424052970203430404577096503401073904.html> [Accessed 19 September 2013]

Warnick, B. (2011) Empiricism, Securement and the New Rhetoric. In: J.T. Gage (Ed.) *The Promise of Reason: Studies in the New Rhetoric*: 21–8

Warren, M.E. (1996) What Should We Expect from More Democracy? Radically Democratic Responses to Politics. *Political Theory*. Published May 1996. **24**(2): 241–70

Wartini, S. and Heriyanto, D.S.N. (2014) Enhancing the Implementation of CSR in Developing Countries to Achieve Sustainable Development: Indonesian Perspective. *US-China Law Review*. **11**: 1022–42. New York, NY, USA: David Publishing Company

Washington Post (2013) Diplomatic Tweets on Rosh Hashanah Inspire Internet Debate in Iran. Published 8 September 2013. Available from: http://articles.washingtonpost.com/2013-09-08/world/41881058_1_task-force-hassan-rouhani-social-media [Accessed 16 September 2013]

Washington Times (2009a) Iran Protest Biggest Since Revolution. *The Washington Times LLC*. Published 16 June 2009. Available from: <http://www.washingtontimes.com/news/2009/jun/16/iran-protest-biggest-since-revolution> [Accessed 10 December 2013]

Washington Times (2009b) Iran's Twitter Revolution. *The Washington Times LLC*. Published 16 June 2009. Available from: <http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution> [Accessed 20 September 2013]

Watkins, A., Papaioannou, T., Kale, D. and Mugwagwa, J. (2014) National Innovation Systems, Developing Countries and the Role of Intermediaries: A Critical Review of the Literature. In: *15th International Schumpeter Society (ISS) Conference*. 27–30 July 2014. Jena, Germany

- Way, L.A. (2005) Ukraine's Orange Revolution: Kuchma's Failed Authoritarianism. *Journal of Democracy*. April 2005. **16**(2): 131–45
- Weber, M. (1922) *Economy and Society: An Outline of Interpretive Sociology*. New York, USA: *Bedminster*
- Wesselink, A. and Hoppe, R. (2010) If Post-Normal Science is the Solution, What is the Problem? The Politics of Activist Environmental Science. *Science, Technology and Human Values*
- Westmarland, N. (2001) The Quantitative/Qualitative Debate and Feminist Research: A Subjective View of Objectivity. *Forum: Qualitative Social Research*. Published February 2001. **2**(1)
- Whitley, R. (Ed.) (1993) *European Business Systems: Firms and Markets in Their National Contexts*. London, UK: *Sage Publications Ltd*.
- Wicken, O. (2007) The Layers of National Innovation Systems: The Historical Evolution of a National Innovation System in Norway. *Centre for Technology, Innovation and Culture (TIK) at University of Oslo*. Published 27 June 2007. Oslo, Norway. Available from: <http://www.sv.uio.no/tik/InnoWP/Wickenhistory%20WPready.pdf> [Accessed 12 October 2013]
- Wilken, R. (2012) Mannheim's Paradox: Ideology, Utopia, Media Technologies, and the Arab Spring. *Fibreculture Journal (FCJ-146)*: 176–203
- Wilkinson, I. (2005) From the Sociology of Risk to a Critical Sociology of Suffering. In: *Draft Paper for Presentation at the Conference of the Social Contexts and Responses to Risk (SCARR) Network*. 28–29 January 2005: University of Kent, Canterbury, UK
- Williams, R. and Edge, D. (1996) The Social Shaping of Technology. *Research Policy*. **25**(6): 865–99
- Williams, R., Slack, R. and Stewart, J. (2000) Social Learning in Multimedia. *Final Report to European Commission, EC Targeted Socio-Economic Research Project 4141 PL 951003*. Published January 2000. Research Centre for Social Sciences / Technology Studies Unit, University of Edinburgh: Scotland, UK
- Wired (2009) Activists Launch Hack Attacks on Tehran Regime. *Condé Nast*. Published 15 June 2009. Available from: <http://www.wired.com/dangerroom/2009/06/activists-launch-hack-attacks-on-tehran-regime> [Accessed 13 September 2013]
- Wired (2013) Iran Blocks VPN Use Ahead of Elections. *Condé Nast UK*. Published 11 March 2013. Available from: <http://www.wired.co.uk/news/archive/2013-03/11/iran-vpn-block> [Accessed 01 September 2013]
- Wired (2015) How a Nation of Tech Copycats Transformed Into a Hub for Innovation. *Condé Nast*. Published 29 December 2015. Available from: <http://www.wired.com/2015/12/tech-innovation-in-china> [Accessed 10 March 2016]

Women's UN Report Network (2010) Iran: Women Online Brave Heavy Internet Surveillance and Risks. *United Nations*. Published 9 April 2010. Available from: http://www.wunrn.com/news/2010/04_10/04_05_10/040510_iran.htm [Accessed 11 September 2013]

Wong, P.K. (1999) National Innovation Systems for Rapid Technological Catch-Up: An Analytical Framework and a Comparative Analysis of Korea, Taiwan and Singapore. *DRUID Summer Conference*. Presented June 1999. Rebuild, Denmark

Wong, P.K. (2003) From Using to Creating Technology: The Evolution of Singapore's National Innovation System and the Changing Role of Public Policy. *Competitiveness, FDI and Technological Activity in East Asia*: 191–238

Woodhouse, E., Hess, D., Breyman, S. and Martin, B. (2002) Science Studies, Activism Possibilities and Problems for Reconstructivist Agendas. *Social Studies of Science*. **32**(2): 297–319

Woodhouse, E. and Patton, J.W. (2004) Design by Society: Science and Technology Studies and the Social Shaping of Design. *Design Issues*. **20**(3): 1–12

Woolley, A. and Malone, T. (2011) What Makes a Team Smarter? More Women. *Harvard Business Review*. Published June 2011. MA, USA. Available from: http://static.ow.ly/docs/Woman%20make%20a%20team%20smarter_pAk.pdf [Accessed 18 December 2013]

World Economic Forum (2009) The Global Gender Gap Report. *Cologny, Switzerland*. Available from: http://www3.weforum.org/docs/WEF_GenderGap_Report_2009.pdf [Accessed 31 August 2013]

World Economic Forum (2012) The Global Information Technology Report 2012: Living in a Hyper-Connected World. Published April 2012. *Cologny, Switzerland*. Available from: http://www3.weforum.org/docs/Global_IT_Report_2012.pdf [Accessed 19 September 2013]

World Internet Stats (2012) Internet Usage in the Middle East: Middle East Internet Usage and Population Statistics. Published 30 June 2012. Available from: <http://www.internetworldstats.com/stats5.htm> [Accessed 01 October 2013]

Wright, A. (2009) ACMA Releases Report on Internet Filtering Technologies and Online Safety Measures. *International Association of Internet Hotlines*. Issue 3. Published 22 April 2009. Available from: <https://old.inhope.org/en/newsletter/issue3/acmaupdate> [Accessed 15 August 2012]

Wu, W. (2007) State Policies, Enterprise Dynamism and Innovation System in Shanghai, China. *Growth and Change*. **38**(4): 544–566

Xindex (2013) Index Policy Paper: Is the EU Heading in the Right Direction on Digital Freedom? *Index On Censorship*. London, UK. Available from: <http://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom> [Accessed 11 September 2013]

- Xiwei, Z. and Xiangdong, Y. (2007) Science and Technology Policy Reform and Its Impact on China's National Innovation System. *Technology in Society*. **29**(3): 317–325
- Yadav, K.P. (2006) Gender Equality and Economic Development. New Delhi, India: *Sarup and Sons*
- Yang, M. (2013) The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response. *North-Western Journal of Technology and Intellectual Property*. **11**: p. 707
- Yardley, L. (2000) Dilemmas in Qualitative Health Research. *Psychology and Health*. **15**(2): 215—28. Taylor and Francis Group, Routledge. Oxford, UK
- Yeates, N. (2008) The Idea of Global Social Policy. In: N. Yeates (Ed.) *Understanding Global Social Policy*. Bristol, UK: Policy Press
- Yim, D.S. (2006) Korea's National Innovation System and the Science and Technology Policy. *Science and Technology Policy Institute*. Washington DC, USA. Available from: http://www.unesco.org/science/psd/thm_innov/forums/korea.pdf [Accessed 10 August 2011]
- Yzer, M.C. and Southwell, B.G. (2008) New Communication Technologies, Old Questions. *American Behavioural Scientist*. **52**(1): 8–20
- Zaluckyj, K. (2012) Orange Revolution: Post-Socialist Urban Political Movement. *College of Liberal Arts and Social Sciences at DePaul University*. Chicago, IL, USA. Available from: <http://via.library.depaul.edu/etd/121> [Accessed 08 August 2012]
- Zehfroush, A. (2012) A Few Words in the Memory of Iranian Revolution February 1979. Available from: <http://antirawuerzburg.blogspot.de/images/AufsatzArashEN.pdf> [Accessed on 06 August 2012]
- Zou, H. and Adams, M.B. (2008) Corporate Ownership, Equity Risk and Returns in the People's Republic of China. *Journal of International Business Studies*. **39**(7): 1149–168

Ethics Approval Certificate

EXTERNAL AND STRATEGIC DEVELOPMENT SERVICES

uel.ac.uk/qa

Quality Assurance and Enhancement



ARASH ANGHAEI
4TH FLOOR, NUMBER 5,
STREET 5/40 NIROOYE HAVAAE, PIROOZI AVENUE,
TEHRAN
IRAN

Date: 7 October 2011

Dear Stewart,

Project Title:	<i>Cyber Activists as Innovators: Online Technology and the Modes of Political Discourse in Iran</i>
Researcher(s):	<i>Arash Anghaei</i>
Supervisor(s):	<i>Dr Josephine Stein</i>

I am writing to confirm that University Research Ethics Committee (UREC) agreed approval for the ethical parameters of your proposed research on Wednesday 5 October 2011.

Should any significant adverse events or considerable changes occur in connection with this research project that may consequently alter relevant ethical considerations, this must be reported immediately to UREC. Subsequent to such changes an Ethical Amendment Form should be completed and submitted to UREC.

Approval is given on the understanding that the 'UEL Code of Good Practice in Research' (www.uel.ac.uk/qa/manual/documents/codeofgoodpracticeinresearch.doc) is adhered to.

Yours sincerely,

Merlin Harries
University Research Ethics Committee (UREC)
Quality Assurance and Enhancement
Telephone: 0208-223-2009
Email: m.harries@uel.ac.uk

Docklands Campus, University Way, London E16 2RD
Tel: +44 (0)20 8223 3322 Fax: +44 (0)20 8223 3394 MINICOM 020 8223 2853
Email: r.carter@uel.ac.uk



Blog Content Analysis Documents

Blog Analysis Questions

1. What is the location of the blogger?
2. What is the gender of the blogger?
3. What is the main focus of the updates?
4. Does the blogger use their outlet as a means to circulate protest/petition/strike calls?
5. What level of computer literacy does the blogger exhibit?
6. Does the blogger use their outlet as a means to share or obtain technical tips about countering the regime's repressive technology, such as how to bypass internet filtering, un-jam satellite TV signals, protect online identities, increase network security or launch hacking attacks on the websites associated with the regime's online police?
7. How many regular contributors does each blog have?

Analysed Blogs

1. Blog title: *Political Humour*

Blog address: <http://tanze30ya30.blogfa.com>

Blog description as written by the author: *This weblog belongs to no particular political personas or parties and is directly run by the enemy itself.*

✓Blog assessment:

Question 1: Unknown

Question 2: Unknown

Question 3: Green movement and/or its leaders, religion and/or superstition, literature/poetry, regime's high-ranking officials and/or key institutions, and technology in relation with filtering and/or surveillance and/or network security

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: More than one (number unknown)

2. Blog title: *Political Humour: Jokes about Ahmadinejad and Khamenei*

Blog address: <http://ba27.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Green movement and/or its leaders, democratic movements in the Arab world, sex, religion and/or superstition, technology in relation with filtering and/or surveillance and/or network security, and regime's high-ranking officials and/or key institutions

Question 4: No

Question 5: Advance

Question 6: Yes

Question 7: One

3. Blog title: *Arman Dekami* (author's real name)

Blog address: <http://g791.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Religion and/or superstition, sports, economy and/or financial transparency and/or poverty and/or subsidy cuts, Green movement and/or its leaders, technology in relation with filtering and/or surveillance and/or network security, and regime's high-ranking officials and/or key institutions

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

4. Blog title: *Alireza Rezaee* (author's real name)

Blog address: <http://alirezarezaee1.blogspot.com> and

http://www.khodnevis.org/persian/author/alireza_rezaei

Blog description as written by the author: *This blog is just about humour.*

✓Blog assessment:

Question 1: France

Question 2: Male

Question 3: Green movement, democratic movements in the Arab world, sports, regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, political prisoners' and/or prisoners of conscience's rights, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

5. Blog title: *Green Iran Forever*

Blog address: <http://greeniranforever.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Toronto, Canada

Question 2: Male

Question 3: Green movement and/or its leaders, religion and/or superstition, literature/poetry, and regime's high-ranking officials and/or key institutions

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

6. Blog title: *Short Messages*

Blog address: <http://tweatter.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Democratic movements in the Arab world, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, political prisoners' and/or prisoners of conscience's rights, women's rights and/or feminism, reformist parties and/or personalities inside Iran, Valentines' day, and sports

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

7. Blog title: *Gameron*

Blog address: <http://gameron.wordpress.com>

Blog description as written by the author: *Nothing in the world is too holy to be critiqued.*

✓Blog assessment:

Question 1: Bandar Abbas, Iran

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, religion and/or superstition, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, reformist parties and/or personalities inside Iran, sex and/or porn, homosexuals' rights, capital punishment, technology in relation with filtering and/or surveillance and/or network security, alcohol and/or drugs, Basij and/or Sundis, elections and/or referendum and/or military coup, civil liberties and freedom of speech/press and/or the Balatarin incident

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

8. Blog title: Mr. Asghar

Blog address: <http://www.asgharagha.com>

Blog description as written by the author: *The first and longest-lasting expatriate journal since the foundation of Islam!*

✓Blog assessment:

Question 1: London, UK

Question 2: Male

Question 3: Literature and/or poetry, religion and/or superstition, sex and/or porn, election and/or referendum, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, reformist parties and/or personalities inside Iran, political prisoners' and/or prisoners of conscience's rights, nuclear power and/or war on Iran and/or sanctions, and technology in relation with filtering and/or surveillance and/or network security, foreign-based satellite channels, economy and/or financial transparency and/or poverty and/or subsidy cuts, and Basij and/or Sundis

Question 4: No

Question 5: Advance

Question 6: Yes

Question 7: One

9. Blog title: *F. M. Sokhan* (author's nickname)

Blog address: <http://www.fmsokhan.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Culture and/or arts, technology in relation with filtering and/or surveillance and/or network security, religion and/or superstition, regime's high-ranking officials and/or key institutions, sex and/or porn, civil liberties and freedom of speech/press and/or the Balatarin incident, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, nuclear power and/or war on Iran and/or sanctions, capital punishment, political prisoners' and/or prisoners of conscience's rights, literature and/or poetry, Basij and/or Sundis, and expatriate opposition parties/personalities

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

10. Blog title: *Seyed Ebrahim Nabavi* (author's real name)

Blog address: <http://www.enabavi.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Belgium

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, Green movement and/or its leaders, students' movement, culture and/or arts, and democratic movements in the Arab world

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

11. Blog title: Nikahang Kowsar (author's real name) and *Nikahang's Musings*

Blog address: <http://www.khodnevis.org/persian/author/nikahang> and <http://nikahang.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Toronto, Canada

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, expatriate opposition parties and/or personalities, Green movement and/or its leaders, culture and/or arts, Valentines' day, reformist parties and/or personalities inside Iran, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

12. Blog title: *Eghbal Mahoori* (author's nickname)

Blog address: <http://www.khodnevis.org/persian/author/eghbaly>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, reformist parties and/or personalities inside Iran, religion and/or superstition, culture and/or arts, and Green movement and/or its leaders

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

13. Blog title: *Mullah Piaz*

Blog address: <http://www.khodnevis.org/persian/author/mullahpiaz> and <http://mullahpiaz.net>

Blog description as written by the author: *Mullah Piaz (onion) lives in modern, troubled Iran. His constant struggle with new technologies and his absurd but logical philosophy make him the remote cousin of Dilbert and Mullah Nasreddin.*

✓Blog assessment:

Question 1: Unknown

Question 2: Unknown

Question 3: Women's rights and/or feminism, religion and/or superstition, culture and/or arts, civil liberties and freedom of speech/press and/or the Balatarin incident, democratic movements in the Arab world, capital punishment and sports

Question 4: No

Question 5: Intermediate

Question 6: No
Question 7: One

14. Blog title: *Mehran* (author's nickname)

Blog address: <http://www.khodnevis.org/persian/author/mehrancartoonist>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, Green movement and/or its leaders, religion and/or superstition, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, reformist parties and/or personalities inside Iran, political prisoners' and/or prisoners of conscience's rights, Basij and/or Sundis, nuclear power and/or war on Iran and/or sanctions, and capital punishment

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

15. Blog title: *Darush Ariaee* (author's nickname), *Uncensored*, and *Persia Royal*

Blog address: <http://www.khodnevis.org/persian/author/darush> ,

<http://sansornashode.blogspot.com> , and <http://persiaroyal.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, civil liberties and freedom of speech/press and/or the Balatarin incident, religion and/or superstition, sports, expatriate opposition parties and/or personalities, democratic movements in the Arab world, Basij and/or Sundis, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, technology in relation with filtering and/or surveillance and/or network security, political prisoners' and/or prisoners of conscience's rights, human rights, economy and/or financial transparency and/or poverty and/or subsidy cuts, and literature and/or poetry

Question 4: No

Question 5: Advanced

Question 6: Yes

Question 7: One

16. Blog title: *Mana Neyestani* (author's real name)

Blog address: <http://zamaaneh.com/zamtoon/cat>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Malaysia

Question 2: Male

Question 3: Torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, political prisoners' and/or prisoners of conscience's rights, women's rights and/or feminism, civil liberties and freedom of speech/press and/or the Balatarin incident, Green movement and/or its leaders, culture and/or arts, and elections and/or referendum and/or military coup

Question 4: No

Question 5: Advanced

Question 6: No

Question 7: One

17. Blog title: *Maatine*

Blog address: <http://maatine.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Culture and/or arts, regime's high-ranking officials and/or key institutions, Green movement and/or its leaders, reformist parties and/or personalities inside Iran, expatriate opposition parties and/or personalities, economy and/or financial transparency and/or poverty and/or subsidy cuts, civil liberties and freedom of speech/press and/or the Balatarin incident, and technology in relation with filtering and/or surveillance and/or network security

Question 4: No

Question 5: Advanced

Question 6: Yes

Question 7: One

18. Blog title: *Rain in the Half-opened Mouth*

Blog address: <http://www.debsh.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Malaysia

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, sex and/or porn, culture and/or arts, literature and/or poetry, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, women's rights and/or feminism, and reformist parties and/or personalities inside Iran

Question 4: No

Question 5: Advanced
Question 6: Yes
Question 7: One

19. Blog title: *In Between*

Blog address: <http://andarmal.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Capital punishment, sex and/or porn, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, nuclear power and/or war on Iran and/or sanctions, Basij and/or Sundis, Sports, religion and/or superstition, economy and/or financial transparency and/or poverty and/or subsidy cuts, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, reformist parties and/or personalities inside Iran, political prisoners' and/or prisoners of conscience's rights, and Green movement and/or its leaders

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

20. Blog title: *What Kind of a Country is This?*

Blog address: <http://mamlekate.blogspot.com>

Blog description as written by the author: *In search of a lost homeland*

And

Blog title: *What is Up Today?*

Blog address: <http://emroozchekhabar.blogspot.com>

Blog description as written by the author: *All the authors are required to be wearing tuxedos while contributing to this weblog.*

✓Blog(s) assessment:

Question 1: Unknown

Question 2: Unknown

Question 3: Sex and/or porn, Basij and/or Sundis, foreign-based satellite channels, sports, economy and/or financial transparency and/or poverty and/or subsidy cuts, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, democratic movements in the Arab world, expatriate opposition parties and/or personalities, religion and/or superstition, culture and/or arts, regime's high-ranking officials and/or key institutions, literature and/or poetry, and political prisoners' and/or prisoners of conscience's rights

Question 4: No

Question 5: Beginner

Question 6: No

Question 7: Three

21. Blog title: *Our Future*

Blog address: <http://ayandema.blogspot.com>

Blog description as written by the author: *Tehran is my Mecca, and this is my notebook.*

✓Blog assessment:

Question 1: Christ Church, New Zealand

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, culture and/or arts, sex and/or porn, Basij and/or Sundis, and expatriate opposition parties and/or personalities

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

22. Blog title: *Tahkhand*

Blog address: <http://tahkhand.blogspot.com>

Blog description as written by the author: *A satirical weblog*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, reformist parties and/or personalities inside Iran, elections and/or referendum and/or military coup, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sex and/or porn, sports, Basij and/or Sundis, nuclear power and/or war on Iran and/or sanctions, economy and/or financial transparency and/or poverty and/or subsidy cuts, and religion and/or superstition

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

23. Blog title: *Today's Front Pages of Newspapers*

Blog address: <http://safhehaval.blogspot.com> and <http://sepehr1970.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, Basij and/or Sundis, civil liberties and freedom of speech/press and/or the Balatarin incident, and technology in relation with filtering and/or surveillance and/or network security

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

24. Blog title: *Mr. Khosn in Exile*

Blog address: <http://blog.hasanagha.org>

Blog description as written by the author: *I am an apostate blogger who believes in atheism.*

✓Blog assessment:

Question 1: Oslo, Norway

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, capital punishment, technology in relation with filtering and/or surveillance and/or network security, religion and/or superstition, elections and/or referendum and/or military coup, economy and/or financial transparency and/or poverty and/or subsidy cuts, nuclear power and/or war on Iran and/or sanctions, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, culture and/or arts, human rights, and civil liberties and freedom of speech/press and/or the Balatarin incident

Question 4: Yes

Question 5: Advance

Question 6: Yes

Question 7: One

25. Blog title: Prophet Yarou (War Be Upon Him!)

Blog address: <http://yaarou.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Religion and/or superstition, sex and/or porn, alcohol and/or drugs, technology in relation with filtering and/or surveillance and/or network security, regime's high-ranking officials and/or key institutions, homosexuals' rights, women's rights and/or feminism, literature and/or poetry, and Basij and/or Sundis

Question 4: No

Question 5: Beginner

Question 6: No

Question 7: One

26. Blog title: *Facetious Sayings*

Blog address: <http://www.hazl.com>

Blog description as written by the author: *Any resemblances to real persons are by no means coincidental.*

✓Blog assessment:

Question 1: California, USA

Question 2: Male

Question 3: Religion and/or superstition, culture and/or arts, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, literature and/or poetry, democratic movements in the Arab world, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, and capital punishment

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

27. Blog title: *Samovar*

Blog address: <http://samavar.wordpress.com>

Blog description as written by the author: *Motivated to create this weblog by my love for opium, I would like to dedicate it to the leader of the Islamic revolution Khamenei from the very south of my heart (somewhere near my colon). Having lived in exile since 1998, I long for a liberal and religion-free Iran, for I think religion is a strictly personal matter.*

✓Blog assessment:

Question 1: Expat, exact location unknown

Question 2: Male

Question 3: Expatriate opposition parties and/or personalities, regime's high-ranking officials and/or key institutions, Green movement and/or its leaders, democratic movements in the Arab world, Basij and/or Sundis, literature and/or poetry, sex and/or porn, nuclear power and/or war on Iran and/or sanctions, religion and/or superstition, alcohol and/or drugs, sports, elections and/or referendum and/or military coup, women's rights and/or feminism, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, economy and/or financial transparency and/or poverty and/or subsidy cuts, and culture and/or arts

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

28. Blog title: *Anti-dictator*

Blog address: <http://zobin-cost.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sex and/or porn, nuclear power and/or war on Iran and/or sanctions, regime's high-ranking officials and/or key institutions, economy and/or financial transparency and/or poverty and/or subsidy cuts, democratic movements in the Arab world, religion and/or superstition, and culture and/or arts

Question 4: No

Question 5: Beginner

Question 6: No

Question 7: One

29. Blog title: *Zekipedia*

Blog address: <http://zekipedia.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Isfahan, Iran

Question 2: Male

Question 3: Democratic movements in the Arab world, regime's high-ranking officials and/or key institutions, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, religion and/or superstition, literature and/or poetry, economy and/or financial transparency and/or poverty and/or subsidy cuts, sex and/or porn, human rights, civil liberties and freedom of speech/press and/or the Balatarin incident, Green movement and/or its leaders, technology in relation with filtering and/or surveillance and/or network security, and sports

Question 4: No

Question 5: Beginner

Question 6: No

Question 7: One

30. Blog title: *Brainless Monkey*

Blog address: <http://brain-less.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: LA, United States

Question 2: Male

Question 3: Expatriate opposition parties and/or personalities, human rights, religion and/or superstition, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, capital punishment, civil liberties and freedom of speech/press and/or the Balatarin incident, Basij and/or Sundis, women's rights and/or feminism, sports, sex and/or porn, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, and elections and/or referendum and/or military coup

Question 4: Yes

Question 5: Advance

Question 6: Yes

Question 7: One

31. Blog title: *Talented Moron*

Blog address: <http://talentedmoron.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Literature and/or poetry, Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, civil liberties and freedom of speech/press and/or the Balatarin incident, sports, religion and/or superstition, capital punishment, human rights, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, culture and/or arts, technology in relation with filtering and/or surveillance and/or network security, alcohol and/or drugs, economy and/or financial transparency and/or poverty and/or subsidy cuts, and nuclear power and/or war on Iran and/or sanctions

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

32. Blog title: *Anger Flame, Shadow of Freedom and Democtatorship*

Blog address: <http://anger-flame.blogspot.com> , <http://freedom-sayeh.blogspot.com> and <http://democtatori.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, religion and/or superstition, Green movement and/or its leaders, democratic movements in the Arab world, economy and/or financial transparency and/or poverty and/or subsidy cuts, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, students' movement, political prisoners' and/or prisoners of conscience's rights, Basij and/or Sundis, human rights, nuclear power and/or war on Iran and/or sanctions, elections and/or referendum and/or military coup, civil liberties and freedom of speech/press and/or the Balatarin incident, culture and/or arts, and capital punishment

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

33. Blog title: *Sight*

Blog address: <http://tanzir-balatarin.blogspot.com>

Blog description as written by the author: *This is where I share my insights about my surrounding issues, giving them a chance to be critiqued.*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, Green movement and/or its leaders, religion and/or superstition, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, economy and/or financial transparency and/or poverty and/or subsidy cuts, culture and/or arts, foreign-based satellite channels, sex and/or porn, Basij and/or Sundis, human rights, women's rights and/or feminism, and political prisoners' and/or prisoners of conscience's rights

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

34. Blog title: *Of Cowardice*

Blog address: <http://bozdelaneh.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, nuclear power and/or war on Iran and/or sanctions, Basij and/or Sundis, economy and/or financial transparency and/or poverty and/or subsidy cuts, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, Green movement and/or its leaders, democratic movements in the Arab world, reformist parties and/or personalities inside Iran, political prisoners' and/or prisoners of conscience's rights, capital punishment, sex and/or porn, culture and/or arts, religion and/or superstition, literature and/or poetry, and technology in relation with filtering and/or surveillance and/or network security

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

35. Blog title: *Serious Humour*

Blog address: <http://werraj.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, Basij and/or Sundis, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, economy and/or financial transparency and/or poverty and/or subsidy cuts, sports, religion and/or superstition, civil liberties and freedom of speech/press and/or the Balatarin incident, literature and/or poetry, and capital punishment

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

36. Blog title: *Amjadiyeh*

Blog address: <http://amjadiyeh1900.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Green movement and/or its leaders, democratic movements in the Arab world, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, Basij and/or Sundis, sports, and capital punishment

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

37. Blog title: *Basiji Jokes*

Blog address: <http://basijoks1.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, Basij and/or Sundis, nuclear power and/or war on Iran and/or sanctions, democratic movements in the Arab world, Green movement and/or its leaders, religion and/or superstition, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

38. Blog title: *Dambooli's Musings: Everything from Everywhere*

Blog address: <http://dambooli.wordpress.com>

Blog description as written by the author: *Dealing with thousands of unanswered questions, I am currently looking for myself. Until a few years ago, I was so religious that never missed a single prayer. I used to listen to the words of the local mosque's Imam so carefully that they would become tattooed in my brain. I would fast every Ramadan, as well as attending all religious ceremonies throughout the year. This all was the case until I began thinking for myself, which I have realised is what the preachers of all major religions work hard to stop one from doing. They say: "listen only to us if you want to go to heaven, and never question our ways, as it is exactly what Satan wants." I am at the moment studying religions, and the more I read, the less religious I become. Unfortunately, I have often found the unreligious to be much more sensible as compared to the religious.*

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Basij and/or Sundis, elections and/or referendum and/or military coup, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, human rights, capital punishment, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, religion and/or superstition, foreign-based satellite channels, Green movement and/or its leaders, women's rights and/or feminism, reformist parties and/or personalities inside Iran, sex and/or porn, civil liberties and freedom of speech/press and/or the Balatarin incident, and children's rights

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

39. Blog title: *Iran's Green movement*

Blog address: <http://irangreenrevolution.wordpress.com>

Blog description as written by the author: *The Iranian people's Green Movement for democracy and freedom*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, expatriate opposition parties and/or personalities, women's rights and/or feminism, children's rights, civil liberties and freedom of speech/press and/or the Balatarin incident, reformist parties and/or personalities inside Iran, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, Basij and/or Sundis, political prisoners' and/or prisoners of conscience's rights, capital punishment, human rights, and foreign-based satellite channels

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

40. Blog title: *Iran Got Ruined*

Blog address: <http://hamid.thepersianland.com>

Blog description as written by the author: *Just another weblog in the land of Persia*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Sex and/or porn, literature and/or poetry, religion and/or superstition, regime's high-ranking officials and/or key institutions, Basij and/or Sundis, women's rights and/or feminism, culture and/or arts, political prisoners' and/or prisoners of conscience's rights, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

41. Blog title: *Dude*

Blog address: <http://melisagodwin.blogspot.com>

Blog description as written by the author: *I have no wish but freedom. Every time a fellow Iranian is killed, humour dies in me all over again, and the smile is wiped off my face, giving its place to a bitter and poisonous frown.*

✓Blog assessment:

Question 1: USA

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, women's rights and/or feminism, religion and/or superstition, civil liberties and freedom of speech/press and/or the Balatarin incident, sex and/or porn, literature and/or poetry, technology in relation with filtering and/or surveillance and/or network security, and economy and/or financial transparency and/or poverty and/or subsidy cuts

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

42. Blog title: *Green Man*

Blog address: <http://sabzemard.wordpress.com>

Blog description as written by the author: *none*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, economy and/or financial transparency and/or poverty and/or subsidy cuts, democratic movements in the Arab world, capital punishment, religion and/or superstition,

torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, political prisoners' and/or prisoners of conscience's rights, reformist parties and/or personalities inside Iran, sports, and women's rights and/or feminism

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

43. Blog title: *Vision is the Truth*

Blog address: <http://visionisthetruth2.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Green movement and/or its leaders, religion and/or superstition, reformist parties and/or personalities inside Iran, civil liberties and freedom of speech/press and/or the Balatarin incident, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sex and/or porn, regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, technology in relation with filtering and/or surveillance and/or network security, women's rights and/or feminism, capital punishment, culture and/or arts, democratic movements in the Arab world, and foreign-based satellite channels

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

44. Blog title: *Green Alliance*

Blog address: <http://ettehadesabz.wordpress.com>

Blog description as written by the author: *I am a secular and liberal green. Green, for me, is a symbol of unification against the fascistic regime in Iran, and does not represent Islamist reformists who only believe in minor democratic changes.*

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, reformist parties and/or personalities inside Iran, economy and/or financial transparency and/or poverty and/or subsidy cuts, literature and/or poetry, culture and/or arts, religion and/or superstition, and technology in relation with filtering and/or surveillance and/or network security

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

45. Blog title: *Green Movement: We Are Countless*

Blog address: <http://nehzatsabz5.blogspot.com>

Blog description as written by the author: *Once upon a time we stood up to get our votes back. But now we are determined to reclaim no less than our well-deserved right to freedom.*

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Green movement and/or its leaders, students' movement, culture and/or arts, literature and/or poetry, regime's high-ranking officials and/or key institutions, elections and/or referendum and/or military coup, capital punishment, expatriate opposition parties and/or personalities, reformist parties and/or personalities inside Iran, Basij and/or Sundis, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, and religion and/or superstition

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

46. Blog title: *Qom's Green Movement*

Blog address: <http://greenqom.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Qom, Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, technology in relation with filtering and/or surveillance and/or network security, culture and/or arts, Basij and/or Sundis, Valentines' day, religion and/or superstition, literature and/or poetry, reformist parties and/or personalities inside Iran, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: No

Question 5: Advance

Question 6: Yes

Question 7: One

47. Blog title: *Green Musings*

Blog address: <http://worldqress.wordpress.com>

Blog description as written by the author: *Today's interesting news and pictures*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, religion and/or superstition, culture and/or arts, technology in relation with filtering and/or surveillance and/or network security, Basij and/or Sundis, economy and/or financial transparency and/or poverty and/or subsidy cuts, capital punishment, and foreign-based satellite channels

Question 4: No

Question 5: Advance

Question 6: Yes

Question 7: One

48. Blog title: *Senaps*

Blog address: <http://senaps.blogspot.com>

Blog description as written by the author: *Analysis of Iran's daily issues*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Culture and/or arts, religion and/or superstition, and economy and/or financial transparency

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

49. Blog title: *Balagari*

Blog address: <http://balagari.wordpress.com>

Blog description as written by the author: *Waiting for you*

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Culture and/or arts, religion and/or superstition, economy and/or financial transparency and/or poverty and/or subsidy cuts, regime's high-ranking officials and/or key institutions, expatriate opposition parties and/or personalities, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, technology in relation with filtering and/or surveillance and/or network security, women's rights and/or feminism, Green movement and/or its leaders, democratic movements in the Arab world, capital punishment, civil liberties and freedom of speech/press and/or the Balatarin incident, nuclear power and/or war on Iran and/or sanctions, and Basij and/or Sundis

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

50. Blog title: *Hollywood*

Blog address: <http://hollywoodweblog.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Shiraz, Iran

Question 2: Male

Question 3: Culture and/or arts, literature and/or poetry, technology in relation with filtering and/or surveillance and/or network security, students' movement, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, regime's high-ranking officials and/or key institutions, nuclear power and/or war on Iran and/or sanctions, sports, sex and/or porn, religion and/or superstition, economy and/or financial transparency and/or poverty and/or subsidy cuts, Basij and/or Sundis, and political prisoners' and/or prisoners of conscience's rights

Question 4: Yes

Question 5: Advance

Question 6: Yes

Question 7: One

51. Blog title: *Mir Ali Sabzineh (author's nickname)*

Blog address: <http://miralisabzineh3.wordpress.com>

Blog description as written by the author: *Every day, I think about what I am capable of doing for the Green resistance of Iran.*

✓Blog assessment:

Question 1: Tehran, Iran

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, women's rights and/or feminism, capital punishment, economy and/or financial transparency and/or poverty and/or subsidy cuts, political prisoners' and/or prisoners of conscience's rights, reformist parties and/or personalities inside Iran, nuclear power and/or war on Iran and/or sanctions, expatriate opposition parties and/or personalities, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, Basij and/or Sundis, religion and/or superstition, and sex and/or porn

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

52. Blog title: *Mullah Hassani*

Blog address: <http://mollah.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Toronto, Canada

Question 2: Male

Question 3: Economy and/or financial transparency and/or poverty and/or subsidy cuts, democratic movements in the Arab world, religion and/or superstition, regime's high-ranking officials and/or key institutions, Basij and/or Sundis, expatriate opposition parties and/or personalities, Green movement and/or its leaders, elections and/or referendum and/or military coup, capital punishment, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, and sports

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

53. Blog title: *Khan Gor's Musings*

Blog address: <http://khangor.blogspot.com> and <http://khangor.blogfa.com>

Blog description as written by the author: *Responsibility has nothing to do with ability; it is instead a product of awareness and ethicality.*

✓Blog assessment:

Question 1: Mazandaran, Iran

Question 2: Female

Question 3: Regime's high-ranking officials and/or key institutions, technology in relation with filtering and/or surveillance and/or network security, economy and/or financial transparency and/or poverty and/or subsidy cuts, civil liberties and freedom of speech/press and/or the Balatarin incident, religion and/or superstition, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, and sports

Question 4: No

Question 5: Intermediate

Question 6: No

Question 7: One

54. Blog title: *Land of Iran*

Blog address: <http://persiatazmin.wordpress.com>

Blog description as written by the author: *Heartfelt scribbles of a brain-dead*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, elections and/or referendum and/or military coup, students' movement, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sex and/or porn, nuclear power and/or war on Iran and/or sanctions, and Basij and/or Sundis

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

55. Blog title: *Moghilan Tree's Thorn*

Blog address: <http://naiem.wordpress.com>

Blog description as written by the author: *Irritating nonsense from a rotten mind*

✓Blog assessment:

Question 1: Australia

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, civil liberties and freedom of speech/press and/or the Balatarin incident, human rights, capital punishment, religion and/or superstition, democratic movements in the Arab world, technology in relation with filtering and/or surveillance and/or network security, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sports, Basij and/or Sundis, nuclear power and/or war on Iran and/or sanctions, literature and/or poetry, culture and/or arts, economy and/or financial transparency and/or poverty and/or subsidy cuts, expatriate opposition parties and/or personalities, political prisoners' and/or prisoners of conscience's rights, and reformist parties and/or personalities inside Iran

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

56. Blog title: *Other Side of the World*

Blog address: <http://onvaredonya.blogspot.com>

Blog description as written by the author: *Denmark is a small country with a very few Iranian citizens as compared to its neighbourhood countries like Sweden and Germany. We, therefore, have a harder time making the world aware of our political activities. Wheels are, nevertheless, in motion here and we are hoping that our activities would be appreciated by the resistance movement inside Iran.*

✓Blog assessment:

Question 1: Copenhagen, Denmark

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, religion and/or superstition, capital punishment, civil liberties and freedom of speech/press and/or the Balatarin incident, culture and/or arts, literature and/or poetry, women's rights and/or feminism, democratic movements in the Arab world, technology in relation with filtering and/or surveillance and/or network security, nuclear power and/or war on Iran and/or sanctions, students' movement, and Basij and/or Sundis

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

57. Blog title: *World of Humour*

Blog address: <http://hosseinpooya.blogspot.com>

Blog description as written by the author: *I have been writing satirical poems and plays for over past twenty years, during which I have been a dedicated supporter of the National Council of Resistance of Iran NCRI). I fight for subversion of the theocratic regime and empowerment of a secular republic in Iran.*

✓Blog assessment:

Question 1: London, England

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, Basij and/or Sundis, literature and/or poetry, economy and/or financial transparency and/or poverty and/or subsidy cuts, democratic movements in the Arab world, technology in relation with filtering and/or surveillance and/or network security, culture and/or arts, nuclear power and/or war on Iran and/or sanctions, Green movement and/or its leaders, capital punishment, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, elections and/or referendum and/or military coup, foreign-based satellite channels, and reformist parties and/or personalities inside Iran

Question 4: No

Question 5: Advance

Question 6: No

Question 7: No

58. Blog title: *Uncle Changiz*

Blog address: <http://www.bipfa.com/amoo-changiz>

Blog description as written by the author: *Don't be scared of my presence, all I'm bringing with me is loneliness.*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Technology in relation with filtering and/or surveillance and/or network security, capital punishment, regime's high-ranking officials and/or key institutions, economy and/or financial transparency and/or poverty and/or subsidy cuts, religion and/or superstition, women's rights and/or feminism, democratic movements in the Arab world, Basij and/or Sundis, sex and/or porn, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, human rights, civil liberties and freedom of speech/press and/or the Balatarin incident, and Valentines' day

Question 4: No

Question 5: Advance

Question 6: Yes

Question 7: One

59. Blog title: *Rebellious*

Blog address: <http://fetnegar01.blogspot.com>

Blog description as written by the author: *I hope to be able to serve freedom of speech by contributing to this weblog.*

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Capital punishment, religion and/or superstition, regime's high-ranking officials and/or key institutions, elections and/or referendum and/or military coup, human rights, political prisoners' and/or prisoners of conscience's rights, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, technology in relation with filtering and/or surveillance and/or network security, Basij and/or Sundis, democratic movements in the Arab world, Green movement and/or its leaders, culture and/or arts, foreign-based satellite channels, and sports

Question 4: Yes

Question 5: Advance

Question 6: Yes

Question 7: One

60. Blog title: *Annamaz*

Blog address: <http://annamaz.blogspot.com>

Blog description as written by the author: *Annamaz is a Turkish word meaning idiot. I am an idiot, because I don't understand people, the logic behind their behaviours, and their habitual misunderstanding of things. This is a place where I write my daily confusions.*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, religion and/or superstition, women's rights and/or feminism, culture and/or arts, Basij and/or Sundis, capital punishment, technology in relation with filtering and/or surveillance and/or network security, economy and/or financial transparency and/or poverty and/or subsidy cuts, and sex and/or porn

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

61. Blog title: *Hidden Sense*

Blog address: <http://chinejan.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, democratic movements in the Arab world, Green movement and/or its leaders, reformist parties and/or personalities inside Iran, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, economy and/or financial transparency and/or poverty and/or subsidy cuts, Basij

and/or Sundis, technology in relation with filtering and/or surveillance and/or network security, culture and/or arts, political prisoners' and/or prisoners of conscience's rights, religion and/or superstition, and expatriate opposition parties and/or personalities

Question 4: Yes

Question 5: Intermediate

Question 6: No

Question 7: One

62. Blog title: *Sober, the Little Prophet*

Blog address: <http://marooned9.blogfa.com> and <http://marooned9.blogspot.com>

Blog description as written by the author: *Ivan Ilyich is thrown in jail; they broke his violin too; but all his family does is bragging about being related to him.*

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Regime's high-ranking officials and/or key institutions, reformist parties and/or personalities inside Iran, religion and/or superstition, culture and/or arts, sports, Basij and/or Sundis, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, technology in relation with filtering and/or surveillance and/or network security, expatriate opposition parties and/or personalities, democratic movements in the Arab world, economy and/or financial transparency and/or poverty and/or subsidy cuts, Green movement and/or its leaders, and sex and/or porn

Question 4: No

Question 5: Advance

Question 6: No

Question 7: One

63. Blog title: *Iran Lover*

Blog address: <http://ashegiran.blogspot.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Unknown

Question 2: Male

Question 3: Green movement and/or its leaders, regime's high-ranking officials and/or key institutions, religion and/or superstition, Basij and/or Sundis, ethnic/religious minorities' rights, culture and/or arts, technology in relation with filtering and/or surveillance and/or network security, and torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

64. Blog title: *Superstition and Broken Clock Hands*

Blog address: <http://khorafe.blogspot.com> and <http://mehdiyaghoubi38.blogspot.com>

Blog description as written by the author: *After the tyrant, it will be time for the oppressed to speak out.*

✓Blog assessment:

Question 1: Expatriate (exact location unknown)

Question 2: Male

Question 3: Economy and/or financial transparency and/or poverty and/or subsidy cuts, regime's high-ranking officials and/or key institutions, religion and/or superstition, sports, women's rights and/or feminism, labourers' rights, students' movement, Basij and/or Sundis, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, sex and/or porn, expatriate opposition parties and/or personalities, literature and/or poetry, civil liberties and freedom of speech/press and/or the Balatarin incident, democratic movements in the Arab world, capital punishment, ethnic/religious minorities' rights, and culture and/or arts

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

65. Blog title: *Dried Whey*

Blog address: <http://kashkmyblog.wordpress.com>

Blog description as written by the author: none

✓Blog assessment:

Question 1: Iran

Question 2: Male

Question 3: Green movement and/or its leaders, democratic movements in the Arab world, regime's high-ranking officials and/or key institutions, reformist parties and/or personalities inside Iran, torture and/or violence and/or detainees' systematic rape and/or the Kahrizak incident, labourers' rights, economy and/or financial transparency and/or poverty and/or subsidy cuts, foreign-based satellite channels, religion and/or superstition, Basij and/or Sundis, sports, culture and/or arts, expatriate opposition parties and/or personalities, literature and/or poetry, and human rights

Question 4: Yes

Question 5: Advance

Question 6: No

Question 7: One

Interview Scripts

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and the cyber-activists in Iran?

The power struggle between the regime and cyber activists in Iran today is no longer a frontline issue because of the manipulation of regime forces on most social networking and its near control of ICT in Iran. The utility of petro-dollar to purchase sophisticated software from companies, such as Nokia or domestically-manufactured technologies that can monitor and control communication, and forcing citizens to purchase only government-approved electronic devices or exchange those they had with newly-government issued telecommunication medium had paralyzed the opposition's ability to mobilise while using ICT as an effective medium. Except for the wide use of Iranian Diaspora for such means, the interconnectedness between citizens within Iran and with Iranian abroad in issues related to confronting the regime is very limited.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

A great deal. Such contributions had strengthened—at least for now—the regime's stronghold on power and caused great damage to democratic mobilisation and town hall-types of cyber meetings. Such pre-emptive strategy at the aftermath of the Green Movement is a lesson to other movements that intend to utilise ICT as an opposition means for popular expression and demonstration of criticism of unpopular policies or political platforms. It also forces researchers to retool in order to better remedy such defects and envision new developments in the cyber frontier in order to counter-balance reactionary regimes' attempts to circumvent the effectiveness of ICT as a mass communication device, especially for democratic movements confronting unpopular policies. One of such innovations, perhaps, is to increase orbited satellites that can offset the function of tyrannical cyber injections, and enable citizens to connect through global cyber balloons when other forums of networking are censored or shut down.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

With worldwide boycotting of Nokia for its role in supporting the Iranian regime in censoring its citizens, the regime was able to overcome Nokia's reluctance to honour full participation by forcing researchers and universities in Iran itself to produce such devices that can do the job—let us call such devices tyrannical cyber injects, or TCI. Although TCI are currently effective in helping the regime in suppressing its populace, the shift may tilt as global awareness demands new innovation in order to maintain an active link in support of human rights and democracy between ICT and cyber activists.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

NSN has caused the case of democracy in Iran and the world a great damage for being the pathfinder in establishing TCI. Such companies—at least their leadership—ought to be accountable for their action not only in the court of public opinion but in international criminal courts. Yes, some may argue that NSN's contract with the Iranian regime was legal within the international business framework. This has to change, especially when regimes such as Iran are facing global sanctions. Businesses no longer can divorce profit from ethics and they have to balance between profitability at all costs, which is a form of piracy, and with that of responsible and ethically-driven conduct. The Iranian regime learned from NSN and adapted its technology in creating its own domestic form of TCI. Thus, NSN cannot escape the judgment of history in supporting the Iranian regime in its attempt to censor its citizens and end all forms of opposition.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

New laws must be adapted that can focus on the following:

- Penalising companies such as NSN who do business with tyrannical regimes and support the suppression of opposition movements or any form of expression.
- Rewarding innovations and companies that clearly support democratic aspirations, human rights and ethics in business.
- Providing funding through loans, grants, and donations for researches aimed to further develop ICT to continue become a viable tool in civic mobility and actions.
- Boycotting, criminalising, and sanctioning all business, researches, and technologies associated with regimes that censor citizens and enforce tyrannical forms of governance against the will of the people.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

There is a return now in Iran to a traditional form of mass communication among activists that utilises small neighbourhood-linked units. The problem with this is that it is too slow, too isolated, and too easy to intercept by regime forces. The lack of political leadership at the opposition adds to the dilemma and leaves anti-regime forces with continuous circulation between despair, hopelessness, looking to the west for an answer or rescue, or surrendering with contempt to the unpopular regime in hope of internal fractions within regime camp that can capitalised on for further development.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

Reality is the mother of all inventions. There is no one particular source and most software used by Iranian cyber-activists are home-made and still lack sophistication to create effective networks. This is where global innovations can help in enabling such network through space ballooning without necessarily having special devices and software available to link with them.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Remarkably, Iranian women are taking the lead in such activities and presenting themselves as experts in finding ways to offset regime offenses through modest, yet determined and continually developing technological solutions to TCI. Especially among them are those educated abroad. The irony, though, even with these leaders' level of expertise, they remain localised because of lack of access to sophisticated technological mediums. This may change as the solutions that they are adapting are increasingly becoming more adaptive.

Any further comments?

ICT is a new frontier in popular movement. It is responsible for the birth of the Global Participant Observer (GPO) and the interconnectedness between people beyond place or particularities. ICT, however, has its many weaknesses and side effects. Among those are the reduction in traditional human/social contacts, increased reliance on technology instead of other scientific explorations and human networking, an increase in individualism at the expense of communal spirit, and saturation of information at the expense of vigorous research and without means to separate between facts from fictions. This is why it was easy for regimes such as that in Iran to manipulate these weaknesses in ICT for its own advantage. ICT and cyber-activism must not relinquish traditional communal and human contacts and use ICT only as a support mechanism to broadcast suppressed voices to the world and maintain internal dynamics. The lessons from the Egyptian and Syrian revolutions ought to be admired. When the Mubarak regime used the same techniques as the Iranian regime is doing now in utilising TCI, opposition forces in Egypt did not surrender to the enforced reality. Instead, they maintained their network through small community units and vigil committees while bridging through mass demonstrations that refused to give up public space. In Syria the same was true and the public space—squares, streets and neighbourhoods—remained filled with demonstrators on daily basis despite massive regime crack down. The opposition remained peaceful for many months, and only when soldiers defected, armed struggles begun in order to protect these demonstrators against regime attacks.

Cyber revolution alone will never work. This is the mistake of Iran's opposition movement. The human presence and voice in the public space must remain defying tyranny in order to make a difference. Only the genuine human voice can be heard, not an electronic version of it. The cyber voice can easily be manipulated, changed or censored. At best, it is nothing but an echo of the human voice. Nevertheless, it is an echo that is effective and can reach far beyond and prevent complete silence when popular movements are crushed. Assad's father

massacred an entire city in 1982 and he was able to get away with it. No one remained alive to witness it and speak out against it, at least no one with a true human decency or conscious inside regime forces. Today, however, his son cannot get away with his crimes. ICT made it impossible for such crimes to go silent into the night. When Assad's henchmen kill innocent Syrian women and children, the next day the whole world is aware of it. They may not do much as global politics still seems to be entangled there while hundreds of thousands are been killed in cold blood, but at least history is a witness with both recorded images and sound. The cyber activists in Iran ought to learn from Egypt and Syria. Although each place has its particularity, tyranny, however, has one common thing: it must be confronted each and every day, in every opportunity, every space, and with every means.

Dr. Babak Rahimi (30 Aug 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and the cyber-activists in Iran?

Mostly government infrastructures but also certain news sites that may be critical of Iranian government.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

We have to distinguish IRGC's private sector and intelligence units within the paramilitary force. It is the latter that are in charge of censorship/surveillance infrastructure.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Since 2010, they have most likely borrowed or copied surveillance technology from Nokia-Siemens Networks and Chinese companies.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

It played a role in the 2009 elections, but since 2010, Iranian surveillance regime has become more domestic-based.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

Prohibiting the sale and intelligence sharing of any computer-related technology that could be used for surveillance purposes.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

VPNs. Widespread and relatively inexpensive.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

Most likely imported from outside of Iran, produced by American and European companies.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

The differences between local and expat are largely a matter of network ties offline, but online is a different matter as the boundaries between outside and inside Iran are broken down between the activists. Yes, gender and age play a critical role. It has to do with generational changes in lifestyle and everyday practices, with technology playing a central role.

Elahe Boghrat (13 Sep 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

Clearly, the regime has more power to disrupt and censor in the virtual world compared to the protesters. On the other hand, as online activism—at least for now—does not usually lead to torture and violent death, cyber activists and human rights advocates have been able to employ modern tools such as social networks and hacking attacks to a considerably useful extent.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

There is no doubt that the above entities altogether spend billions on complex technological infrastructures to sniff [out] and neutralise online dissent. Therefore, the more the protesters turn to the internet as a means of political activism, the more funds and human resources will be required by the regime to fight back. This is indeed challenging for the government given the on-going economic sanctions imposed on it by the west. Under such circumstances, the only option left would be for the regime to take a more radical, North-Korean-style censorship approach, which is exactly why it is now speaking of replacing the internet with a 'halal' (filth-free) network. But even this looks currently far from feasible due to the sanctions and gradual collapse of the country's economy. The regime is now forced to a point where it has to prioritise its expenses and online censorship is being pushed back in the queue by the more vital—and extremely costly—operations such as street crackdowns nationwide and various secret governmental projects.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

The regime itself always insists to convince everyone that they are entirely independent and reliant on in-house scientists and scientific innovations. That is while not even the technology but often the technicians the government speaks of are rented from the west either lawfully or illegally. Of course, there are also some Iranian scientists working in the area, as even the imported—or in many cases smuggled—knowledge or equipment need to be handled by experts and will be wasted otherwise.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Corporations are not founded on humanitarian grounds and are not there to simply help the democratisation process in underdeveloped countries! Instead, their main goal is always generating profit, and the identity of the buyer doesn't really play a role in their big business decisions.

The only time such companies may avoid transacting with dubious entities is when they are pressurised by their governments—which hardly happens in democratic countries—or by their people in such a fierce way that they see the deal as a serious long-term threat to their overall business—e.g. boycotts in the overcrowded Middle-Eastern markets, hefty fines, etc. At any rate, the Iranian regime's extensive relations with foreign companies show the emptiness of their self-reliance claims!

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

Due to legal complications caused by complete independence of many Western trading companies from their respective governments, neither the individual governments nor the EU can really force any companies into or out of business with anyone. All they can do, therefore, is to advise them on the consequences and hope for such advice to be reflected in their business decisions.

Sanctions, however, work completely differently. When it comes to sanctions, corporations are simply forced to abide by the rules or else they will have to face the consequences. The fact that even Iran's Supreme Leader has recently called the sanctions "sadistic" shows how seriously such efforts—again, despite the regime's independence claims—have hit the country's economy, particularly the government's financial resources. The embedment of ICT-related knowledge and equipment into these sanctions can cause the regime many big troubles.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

Anti-filtering software, along with the fluid/viral nature of online activism, can certainly help the opposition movement to sustain. However, I personally find satellite radio and TV more effective on the country's socio-political discourse. This is mainly due to the mainstream Iranian public's lack of access to either the internet or sufficient technical knowledge to help them make proper use of it.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

I am not aware of the identity of those involved in the development of such software. But these tools have always found their way to the Iranian netizens, assisting the growth of a democratic culture within them. Unfortunately—due to politically-motivated censorship on the regime side—the internet is widely viewed among Iranians as an exclusively political instrument and there is hardly any elaboration done on its social, cultural and economical influences, or even its negative impacts on certain things!

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Naturally, expat Iranian activists are more successful in establishing a dialogue with their audience as compared to their native counterparts, due to [the] liberal nature of the Western countries where most of them reside. With regards to age and gender, while I'm sure they are quite influential, I can't say much as there are no scientific surveys or statistics published on this specific issue.

Any further comments?

Given what we have been through, and regardless of our geographical location, we Iranians tend to react rather emotionally—instead of rationally—to certain events both in the online and offline worlds. Therefore, I, for one, take the Iranian online political scene for what it is and refuse to make more of it than I believe I should. This opinion is formed particularly based on my experiences as a professional journalist with the internet over the past five years.

Dr. James Fielder (30 Aug 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

My assessment is that cyber-activists have leaned significantly more towards social networks rather than hacking. Maintaining reliable communication channels appears more important, and the hacking that's employed is used to evade censors rather than to carry out offensive attacks. Social networking sites such as Twitter and Facebook are particularly useful in that they allow users to broadcast real time information to thousands, particularly expatriates and outside audiences.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

In truth, in my research I never found specific development links to the IRGC or Iranian universities. As researchers worldwide say: gads, I'd better go Google that real quickly and make myself look smart!

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Iran is largely self-sufficient. Speaking broadly, Iran, in my experience, has been fairly successful at producing a wide variety of defence-related materiel despite the long-term embargo, particularly small arms, aircraft parts and even the Zulfiqar tank. Even with an embargo, Iran has access to significant resources and [the] resilience of a mixed economy, in contrast to oil rentier states such as Saudi Arabia. In addition to embargo limitations, Iran also seeks self-reliance in order to avoid risks associated with foreign company software security holes, particularly deliberately installed backdoors.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

NSN in particular claims to have only provided cell phone-tapping capability. In 2009, ONI reported that US company Secure Computing provided Iran filtering software, based on electronic forensics, but the company denied doing so. I have some sympathy for the companies, in that their primary mission is to sell products. Altruism sounds good, but is bad for the balance sheet! In addition, should ICT companies be held liable for how regimes use legally purchased products? That's a question I can't answer. I'd personally be in a moral quandary if I were working for a company that made all decisions solely on sales with little regard for ethical decisions.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

In contrast to the layers of profit/ethical issues discussed previously, purposeful evasion of multilateral sanctions is a different matter. In those cases, the companies in question should be held accountable for contracts made after sanctions are placed. Some observers may argue that international legislative bodies lack sufficient enforcement capabilities, and the efficacy of sanctions suffers when states don't cooperate. That said, I assess that international forums are the best place for states to come to unified agreement. Thus, while the European Parliament may lack direct coercive authority, it—and other IGOs—can apply incredible political influence that ultimately pressures states to toe policy lines.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

Activists typically use VPN connections, specific tools such as the TOR network, BitTorrent, and Simurgh, and other various proxy servers to evade censorship (both blocking and surveillance). I underline "various" since Simurgh is technically a proxy software program created in Iran. However, there are a variety of hardware and software proxy server solutions such as CC Proxy and EZ Proxy. I even once experimented with an embeddable html proxy script—the file name escapes me. Basically, the only practical and reliable method to evade Iran's censorship regime is through an unblocked proxy server. It becomes a game of cat and mouse between the activists and the regime, with the activists finding or building new proxies as Iran's Ministry of Communications and Information Technology sniffs them out.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

With the exception of Simurgh, anti-censorship/surveillance software is Western-made; at least, Simurgh is the only home grown product I'm aware of. In addition to software, activists can access overseas hardware proxies directly, typically through a simple web or numerical IP address. Numerical addresses are often more reliable, as they don't trip keyword filters. My understanding is that numerical IP proxies eventually fail once censors identify increased traffic to and from the address.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

I think expat influences are grossly overlooked; indeed, I saw it as a weakness in my own dissertation! Expats serve two primary functions: as information sources for local activists and as broadcasters to overseas audiences. I also assess that the link between urban locals and expats are more crucial than links between urban and rural locals. A vigorous information pipeline depends on not only a robust network but also educated and savvy users, both of which are more likely in urban centres. I definitely assess that younger users are more likely to be cyber-activists, again particularly well-educated urbanites. For younger users, the 1979 revolution is, at the very least, a dim memory. Indeed, [for] those my age (late 30s) the

horrors of the Iran-Iraq War probably carries greater emotional weight. As for even younger users, they have no personal knowledge of either event. Thus, younger users are less likely to have an emotional stake in the revolution. Moreover, having grown up with increased ICT access, I assess younger users are more likely to be ICT savvy than older cohorts. I also assess that both young men and women are equally likely to engage in cyber activism, particular in urban areas. In addition to less ICT in rural areas, I also assess greater conservatism and fewer educational opportunities create larger age and gender cleavages.

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

I think social networking can be a powerful tool for social change, but only if the people using social networking sites are protected in terms of their anonymity. Unfortunately, with weaknesses in the Certificate Authority system it's no longer the case that activists can know for sure that they're talking directly to, e.g., Facebook or Gmail's servers when they use the internet. The government could be using man-in-the-middle attacks to steal their username and password and then monitor their activities and tie particular people to specific social media posts. Without a basic level of trust, it becomes difficult for activists to use social media sites outside the country. I don't have any specific comments about politically motivated hacking attacks.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

I don't know anything specific about this other than what I've read in the media and heard from others, the main thing being that Western companies built a centralised routing infrastructure for Iran where they can observe and manipulate any international traffic in fairly advanced ways.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Again, I don't have any specific information about this. I think the Iranian government has demonstrated some serious innovation in terms of making the best use of the capabilities they have. Attacking the Certificate Authority system was a huge blow to those who are fighting for human rights in Iran, in my opinion, because the basic level of trust on the internet that you're really talking to a particular Western company and not to someone in the middle when you use the internet basically fell apart.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

I only know that they reportedly built the system in Tehran that is used as a chokepoint for the internet, and that this chokepoint is critical because it makes man-in-the-middle attacks relatively easy to implement. Few other countries have that kind of capability.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I don't necessarily advocate government interference on the internet or in the Certificate Authority system, but an issue the government should be aware of is that when a dissident in a country like Iran downloads an operating system and/or web browser, there are trust relationships built into that. For example, if you download Firefox there are about 70 companies that Firefox trusts to sign certificates and authenticate websites like Facebook and Gmail to you. Several of those 70 companies were not trustworthy and were basically hacked by someone who was possibly affiliated with the Iranian government. This meant that for at least a short period of time internet users in Iran who thought they had a safe, encrypted connection to sites like Facebook and Gmail could have been in fact communicating directly with an Iranian government server in Tehran that was designed to, for example, collect usernames and passwords. If social media is to be an instrument of social change in places like Iran, we need a better notion of trust on the internet. Funding research in this area is one thought that comes to mind in terms of what the government could do.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

I'm not the right person to answer this question. The TOR project may be the right people to contact if you'd like an answer to this question.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

Again, this is outside of my research area and I'm not able to answer this question.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

My research is mostly about internet censorship in China, so I can't answer this question.

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

The topic area you ask about is perhaps the area of most interest for me. Not just as they relate to Iran but in general. The advancements in the use of social media by special interest groups and virtual organisations are substantial and growing. They can communicate both overtly and covertly, recruit followers, coordinate activities and get their message out to the masses.

In fact one area of research I am currently involved in is the emergence of virtual states. My current and generally accepted working definition of a virtual state (VS) is a nebulous community of people that self-identify and share a common social, political and/or ideological conviction, ideas and values. The VS is unbound by geographic specification. Virtual states are directed by administrators that are charged with coordinating the establishment of the entities overall course based on the motivation of the community. Once the course is established, their efforts are to influence or force governments, nations or other identified groups to change; to align with the virtual state's social, political and/or ideological convictions. Hacking is just one of many cyber-weapons and tools that a VS or group has at their disposal to influence another entity.

I believe the internet has become the primary medium of interaction for a vast number of people worldwide. Messages are coded and hidden in interactions that take place over the internet routinely as well as in your face marketing and positioning campaigns. It has somewhat levelled the playing field between well-established large entities with significant resources including money and groups that have far fewer assets. The struggles inside of Iran as well as other areas of conflict and disagreement are examples of the power hacking and social networking sites bring.

★ General social networking sites' power as demonstrated to date:
- Would rank a 4.0 with a potential of 4.4 (1 = Low, 3 = Medium, 5 = High)

★ General Hacktivism Power as demonstrated to date:
- Would rank a 3.5 with a potential of 4.2 (1 = Low, 3 = Medium, 5 = High)

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Given the unique characteristics and resiliency of virtual states and those that closely resemble the cyber-activists in Iran, self-reliance does not matter. It is like they are shooting bullets into the air. There is nothing really to hit until they (VS or cyber activists) strike and most of the time it is with infrastructure assets outside of Iran's control—often in another country. If Iran were to strike the cyber infrastructure assets of the cyber activists in another country—that would be very dangerous!

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Cyber-activists and most virtual states for that matter are quite resilient due to their architecture and the fact they operate without being tied to any physical location or technology or piece of communications infrastructure. They are typically vendor agnostic! So any actions that focus [on] a specific type of equipment would have limited impact. I am aware that there are multiple investigations into telecommunications firms that allegedly conspired to illegally ship hardware and software purchased from US tech firms and others to entities inside of Iran which is a violation of several US federal laws and a trade embargo imposed on the outlaw Islamic nation. So I will not comment further.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I believe they have already through sanctions and through the export restrictions! Are there those that work to circumvent these controls—YES, and they will pay the price once they are discovered.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

The most common cyber-operations modality that best illustrates virtual states and cyber-activists is a semi-filled balloon. If you apply pressure with your finger in one place—it just pushes outward in other areas. This is the basic architecture of virtual states and most activists. Even though the cyber-activists you are interested in—[are] heavily concentrated (physically) in Iran their membership reaches around the globe. Most cyber-activists have an operational model similar to that of a virtual state. The appearance of the cyber-activists in Iran is much closer to a real virtual state than other groups.

Any further comments?

Given how closed the Iranian environment is to the outside world—there is an absence of facts and only opinion!

Layla Hashemi (31 Aug 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

Social networking has become a key component in Iranian politics not just because of its power as a medium of expression, but more so as an extension of the use of traditional media as a platform for socio-political claims by the public. Iranian women involved in the likes of the Equal Rights Campaign utilised social media tactics learned from Tunisian women, and the entire phenomenon we regard as the Arab Spring continues to learn from its neighbours/peers and collaborate as they plan events and protests.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

The Iranian government clearly has its act together when it comes to utilising ICTs to its benefit. Through either direct or indirect means, the state has both recognised the power of technology and harnessed this power to cater arenas such as the world wide web to its specifications and interests, whether this be through the establishment of government funded websites and weblogs or through censorship of information.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

They have complete control because they own and control everything.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

While the primary force for change should ideally come from within a country, the growing influence of foreign telecommunications companies is an essential factor in defining the future boundaries of Iran's—as well as every other nations'—cyberspace. A good example of this is Haystack in Iran or Google Inc. in China. We are increasingly at risk of losing what is now seeing as one internet. After the recent media hype over the controversial film *Innocence of Muslims*, the debate over freedom of expression within cyberspace has reached a new level: one where religion and cultural traditions are seemingly the main ingredients. But as demonstrated by online communities such as #Occupy, anti-SOPA/PIPA groups and Anonymous, internet users are not about to give up their freedoms so easily. These individuals are young, tech-savvy, and constantly on the move—as some like to say, they have "no return address." At the end of the day it is much too difficult, and not to mention

costly, to stop the hacker who is helping hide IP addresses for political activists or contributing to the takeover of a state or corporate-run website. The 21st century state faces an increasingly sophisticated, resource-rich, and untraceable adversary. While many scholars have previously questioned the waning power of the state, contemporary technologies are giving non-state actors—as well as their respective governments—some of the most powerful tools they've had yet. The resulting cyber wars between and within nations will define how conflict is played out in this century.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

This is a tough question, because the first thing I'm tempted to ask is: should they or do they have a right to intervene at all?

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

In addition to being one of the first nation-states to utilise the internet to disseminate information about presidential candidates, a variety of online tactics [have been] used by both the Iranian public and the state since the initial appearance of the technology in the country at the turn of the 21st century. These actions are commonplace and practical for all parties involved; to be technologically 'with it' these days is deemed as critically linked to public opinion and activism. Any state would be wise in trying to harness a developing technology as powerful as the internet. In fact, any state not trying to do just that is doing itself—and arguably sometimes its people—a great disservice.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

Are we referring to filter breakers here? I don't have much knowledge on the subject but it makes me think of all of the illegal satellite dishes in the country and various online dissent groups. To a certain extent, breaking censorship laws is almost accepted as a petty crime as it is often portrayed in Iranian media and pop culture as being something practiced by Iranians of a wide range of socio-economic strata.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Regardless of the country in question, I believe that the call for political change should and must come from within the nation.

That being said, I feel there is a large, young Iranian expat community that longs to reconnect to their homeland. New social media and the internet in general have become great resources to meet this end. Whether it is catching up on the latest musical, cultural or fashion trends in Tehran or keeping in touch with a distant relative in Khuzestan or Kansas, tools like Orkut or Facebook make these tasks much more feasible for both the native and expat Iranian.

With regards to gender, while I do not have much first-hand experience, through research I have learned that many Iranian women both inside and outside of the country use aliases online to disguise their gender. While much can be said about this phenomenon, I think it is important to both recognise and attempt to dissect the reasoning behind such actions in order to fully address global equality and general gender roles and norms.

Any further comments?

In this age of globalisation, many second-generation Americans have developed an identity crisis, and young Iranians growing up in foreign—mostly Western—countries are no exception. Often upon sharing that you are Iranian or Iranian-American, the first response you get is horrified or deeply strained facial expressions and the occasional "is it safe over there?" With all of the misperception and lack of information, it often becomes difficult to successfully counter-balance the Western media's clamour about the axis of evil, uranium enrichment, and the on-going "war on terror." The reality is that the majority of the world's citizens do not know enough about politics—or the current global nuclear arms race—to make an informed decision or opinion about Iran. The unfortunate result is that many people in the world perceive these "rogue nations" as dangerous and untrustworthy, further feeding into what we in International Relations call the security dilemma. These perceived images of the "evil other" have the darkest corners of history, but the potential for misinformation increases parallel to the increased frequency and volume of information accompanied by new social media. Also, with the emergence of the internet meme culture, many of these perceptions have been overly simplified and made easily digestible through the use of infographics and humour, making these myths of "the other" easier to swallow for any audience. As much as I would love to say that new communications technology like the world wide web will turn this destructive, self-help system around, that would be like saying that by having a hammer, one is in sufficient a situation to build an entire house from scratch. Nothing good comes without hard work, and the idea of liberal democracy seems too appealing to come easily for any country.

Madeline Storck (03 Sep 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and the cyber-activists in Iran?

The media latched on to the catchy phrase 'Twitter Revolution' to describe the trend across the Middle East of young and techno savvy activists using the internet as a weapon against authoritarian and repressive governments. However, this impression relies on broad assumptions about the democratic nature of the internet, ignoring the importance of context, both cultural and historical. The Iranian government is known to have one of the most advanced systems of networked authoritarianism in the world, perhaps second only to China. The internet is a dialectical force, and though recently its potentials for strengthening pro-democracy movements have been given much attention, when monopolised by an authoritarian state, it has equally dire consequences. My understanding of the political situation in Iran is superficial, but I would argue that so far, since the 2009 elections and more recently in the events of the Arab Spring, social networking has played a significant role in three ways: as an organisational tool for networking activists, as a means of generating awareness in the international community of the events taking place in authoritarian countries, and finally as an alternative press. The rise of citizen journalism has altered the traditional state-based monopoly over information.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Though technology used to track down activists was sold to Iranian mobile phone companies by NSN, the programmes are not considered unlawful—this was determined at a European Union hearing. This has also happened with a system by Ericsson sold to Belarusian mobile phone operators. In European countries, the same lawful intercept technology is used to track criminals. However, in the Iranian example, the definition of criminal is clearly being stretched.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

While I don't know if this is the case in Iran, in the Egyptian example, local cyber-activists played an important role in planning and organising protests, while expat cyber-activists' role was more in generating awareness in the wider world of the events taking place within the country in question. During the 2009 elections in Iran, social media users provided an important source of information for the US government. The US and Iran have had no formal diplomatic relations for three decades, and thus, new media has proven to be an outlet for information not only to citizens of Iran but the wider international community. Regarding age and gender, I would say that both can be determining factors in activists' use of new media.

Though use of social media, blogging in particular, has increased dramatically in the last decade, I would argue that it is important not to forget about the digital divide. I came across this trend while researching my dissertation. It is easy to assume that the dialogue taking place via social media is representative of the wider anti-government movement. However, this is often not the case. When interviewing Egyptian students for my own research, they constantly reiterated that most internet users are usually young, educated, often speak English and usually from cities. Therefore, we are hearing from a small percentage of the population, relatively speaking.

Dr. Marcus Michaelsen (30 Aug 2012)

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

Iranians are one of the biggest user groups on TOR—I've heard the number of 50,000 daily. This concerns not only the activists but also the ordinary people seeking to access different kinds of blocked content. Someone from TOR told me that the Iranian authorities are not very successful in discovering connections to the TOR network and that the TOR people were able to quickly counter the few attempts made with deep packet inspection.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

As for the sources behind anti-censorship software, I still believe—and maybe I'm being naive here—that support mainly comes from activist networks and individuals outside Iran who have the motivation, expertise and knowledge to fight censorship. They might get funding from some governments and institutions, but I am not really sure if the US or the European countries have any substantial programmes or long-term budgets to help the activists in Iran.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Some cyber-activists told me that Iranian activists from inside the country are very capable of finding ways to counter filtering and censorship. I don't know about the networks and cooperation between exiles and activists in the country. There are definitely exiles engaged in hacking and attacks against regime websites, though the question would be if/how people inside the country have the technological capacity and infrastructure to participate.

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and the cyber-activists in Iran?

With regard to social networking, I believe it is important to distinguish between the value of social networking in helping disseminate truthful news reporting of so-called dissident Iranian activity to audiences outside of Iran—something that is no doubt of great value to Iran's civil rights movement—and the value of social networks in helping to facilitate pro-democracy cyber activity within Iran. It's my understanding that social networking is not nearly as powerful a tool for mobilising social movements within Iran as it is in Europe or the US. It's simply too dangerous for individuals within Iran to expose their political leanings on networks like Facebook. Politically motivated hacks, on the other hand, are a valuable tool in the Iranian cyber-activist's arsenal. It goes without saying that Iran's theocracy is, like all modern governments, increasingly dependent on networked technology and as such grows increasingly vulnerable to cyber-warfare with each passing day.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

Unfortunately, I cannot claim to have specific information on this point. Nevertheless as a general matter, we know that the regime has a hand in virtually every profitable venture and as such is able to attract the best and brightest of Iran's remarkably well-educated populace. Iran's universities and businesses are just as captive as the average Iranian citizen, and so we have every reason to believe that their best minds are being plundered in furtherance of the regime's censorship and domestic surveillance schemes.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

This is a very difficult question and honestly I doubt if anyone could answer it with any accuracy. The regime is very good at hiding the inner workings of its domestic surveillance apparatus. That said, I believe we have decades of evidence indicating that the regime is quite adept at copying—and improving—technologies originally developed by others. It's a scrappy sort of self-reliance and I would be very surprised if the regime was not largely self-sufficient at this point.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Again, this is an extremely difficult question for the reasons explained earlier. If I had to guess, I would say that the regime's reliance on formal relationships with foreign telecom and technology companies is a red herring. Iran does not need formal business arrangements to acquire foreign technology. It's important to remember that Iran does not abide by any patent or copyright norms. There is nothing to stop it from appropriating whatever technology it requires.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I cannot overemphasise the importance of sanctions. Iran can steal digital technology because it is easy to copy. But Iran cannot steal everything, and it is highly dependent on all manner of imports, from refined fuel to airplane parts. It has become fashionable of late to decry sanctions as only harming the Iranian people. I fear that the intelligentsia who circulate this common lament have handed the regime a gift on a golden platter. The regime simply loves to spin the sanctions as a tool of the evil West, thereby inflaming the famous passions of a prideful Iranian populace and in the process totally avoiding all discussion of what actually led to those sanctions: the regime's own actions. The world has underestimated the Iranian regime's shameless taste for demagoguery and the blinding national pride of its people. Sanctions are, quite simply, an efficient way to cripple this regime and end Iran's decades-long occupation under an unelected and oppressive theocracy.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

Cyber-activism is a dangerous business in Iran. They evade detection and circumvent censorship primarily by routing traffic through proxies and masking their IP addresses—methods that are cumbersome even on high-speed internet connections. I believe network latency is the main reason that technologies like Tor, for example, are not more widely used within Iran.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Local cyber-activists are probably smaller in number than their expat compatriots, but the former's actions have a greater immediate impact on the regime. I don't mean to belittle the role of expatriate activism—indeed I would count myself among that group. But expats have a very different role to play. They are the true ambassadors of the Iranian people and their voices are influential in shaping public opinion abroad. It is hard to measure the direct in-country impact of cyber-activism abroad, but to the extent that local activists continue to rely on proxies, traffic routing, and other technologies that funnel data through network connections outside of Iran, expats—and other netizens—can aide local Iranian activists by simply donating a bit of bandwidth on a volunteer-run anonymity network like Tor. I am unaware of any gender or age effects in this regard.

Neal Ungerleider (21 Sep 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

I argue that social networking's most important role is connecting the Iranian activist diaspora—and their sympathisers—with Iranian cyber-activists. YouTube, Facebook, Twitter, and Skype are infinitely better tools than telephones or snail mail.

The Iranian regime, from what I have seen—and I recognise this is as a non-Persian speaking Westerner—seems to be more interested in stifling social networking than attempting to win the hearts and minds of cyber-activists via social media.

Hacking attacks—DDoS, malware and phishing attacks—against cyber-activists are common at the hands of the Iranian government and regime supporters. With that said, they seem to be on the decline. It's easier to use filtering software or pull DNS malarkey than to do unsophisticated hacker attacks.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Not self-reliant at all. Even the USA, the world's arguable leader in software, routinely uses foreign-created software in their own—private sector—net-filtering or cyber-warfare efforts. Iran has plenty of talented coders, engineers and IT folks, but there are too many structural issues preventing a 100 per cent home-grown internet censorship regime.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Massive. As a journalist, I'm not comfortable going on the record without solid evidence of illegal sales of surveillance technology by EU and American firms to the Iranian government or to government-affiliated companies. With that said, Privacy International has done impeccable research on the subject that speaks for itself.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

Stiff sanctions and fines. I'd argue that the onus is not on the European Parliament, but on individual governments—UK, Germany and Italy especially—to put pressure on firms to adhere to existing but loosely enforced laws.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

Everything from HTTPS to Tor to burner phones to VPNs. I would say they're commonplace but not practical—the learning curve around many of these tools ensures only techies use them.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

[The] main source behind development is the ethos of the hacker and techie culture—the idea of information being free at all costs and moral opposition to censorship. Funding of development, however, is another story. I would argue it is a mix of idealistic individuals, companies hoping to later monetise these technologies in different contexts, and government actors—US and EU—embracing the Iranian opposition for their own interests.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

The overwhelming majority of Americans opposes the current drift toward war and laments the hostile behaviour of Israel, Iran, and the United States. The parliaments of all democratic countries should work urgently to deepen cultural and educational ties between their peoples and the people of Iran. They should stress 'people to people' contacts, such as exchanging students, community leaders and religious groups. Legislators should increase government spending on research and development aimed at deepening our knowledge of internet issues in Iran, China, Russia, Syria and other countries where cyber-activists are being suppressed. Clearly, legislation is needed to regulate the behaviour of our telecommunications companies in Iran and elsewhere. They should not be allowed to help autocratic regimes monitor, harass, and suppress their own peoples.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Definitely not too much. You are, of course, aware about the European and Chinese technology, which [has] been offered to the regime especially in 2009 and 2010.

Regarding China, perhaps we cannot blame them so much, because they never have claimed that China is a democratic or pro human rights state but in Europe, [where] human rights are considered as a basic issue, the governments did not show a strong reaction against the companies which offered Iran's government the technology to trace the activists.

So it makes the people more disappointed that always the priority is economic interests for European states and practically human rights values [are] mostly a verbal game.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Offering the technology to Iranian authorities to trace the activists and repress the demonstrations quickly.

But we need to consider this issue that Persian people also are not united to follow such cases seriously and systematically. I mean, following the cases through legal organisations. Those who are inside practically are not able to do something effective and those who are outside mostly think of their own interest. The controversy remained mostly on a media level, and did not go much farther.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

They can be quite effective, but in my opinion the priority is economic interests, not supporting human rights movements in Iran. As far as they do not change this policy we can't be hopeful to change things through EU.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Those who are outside, freely and quickly spread the links and news; the materials coming from the insiders, I mean. But those who are inside, their priority is transferring the data in a safe way, but at the same time their views on the situation can be more realistic because they are inside the country.

Any further comments?

Years after the 1980s, it was finally revealed that many Western governments who seem pro human rights were aware of providing Saddam Hussein with products used in making chemical bombs. Nothing happened. Same will happen about the 2009 demonstrations in Iran. Although parts of the story like the Nokia incident or the German torture equipment have been already revealed.

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

I am not entirely sure what you are asking here, but I will take it to mean how influential do I perceive each of these to be.

As to social media, I think that in and of itself, social networking is not all that important. It can be used, however, to develop networks of resistance, as it were, but only within certain conditions. It does allow people to recognise others with like motivations and intentions, and thus can be a powerful organisational [and] mobilisation tool.

As to hacking, I think this can be pretty important, depending upon the skill and number of hackers. Most hacking is primarily symbolic, and has no real function other than to say: "we were here." But hacking that began to undermine governmental effectiveness or the ability of the government to control public narratives could be very important in undermining public support.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

I am not an expert on Iran, so I can't speak about Iran specifically here. However, generally speaking and in other authoritarian regimes, these partnerships between the government and government financed organisations are critically important.

In China, for example, GLCs (government linked companies) have had tremendous impact in changing the actual hardware/software configurations of technological infrastructure components, allowing the government to more or less dictate surveillance capacity at a level that was not heard of a dozen years ago.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Again, I can't speak directly to the Iranian situation, but my guess would be that they are not very self-reliant. I know there is an ongoing investigation into the relationship of China's IT manufacturers, such as Huawei, and the Iranian government. The economist had a recent article on Huawei's recent ascent in the global IT marketplace, and China's government historically would support that kind of partnership. So, Iran does have some tech capacity, both in manufacturing and programming, but I don't think it would need a tremendous amount to mount a successful surveillance regime.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

I cannot speak to European companies. I wouldn't think that the European companies would be that important, given my earlier comments.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

There is not a tremendous amount of leverage the EP or other global bodies can [have] here, other than [via] some symbolic moves. If they try to impose strict controls on European or US involvement, then the Chinese will fill the hole.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

I cannot speak specifically to this, since I don't have contacts myself within Iran. I do know that the TOR project, Haystack, and others like it, have their origins in the work of many European and US-based project groups.

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

I wouldn't exactly call it a power struggle. In my view, that is the least of the cyber-activists' concerns, because it all is overt and the activists can take appropriate precautions to be prepared for hacking, etc. I think that infiltration is a more serious issue to the cyber-activists, which is often achieved through politically motivated hacking attacks.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I don't think if censorship should be selective. It should be banned in all countries. Hence, there should be policies to prohibit contributing to censorship in any way by the information technology industry.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

Yes, gender and age do play a role in choosing the internet as a medium for communication. The young people tend to be more computer-savvy, and women with children find it more convenient to connect with others via the web.

Dr. Tessa Houghton (14 Sep 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

I would say that out of the two, social networking sites—in my opinion—represent a greater potential threat to the regime than hacking attacks, purely because of the fact that they have the potential to facilitate organisation and solidarity amongst much greater numbers of people than single instances of hacking attacks—by hacking attacks, I assume you are referring to DDoS or defacements. However, the problem, of course, is that they can be blocked, and their owners can sometimes be implicit in any censorship imposed by the regime.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

I really don't know a lot about this issue re: Iran, so don't have much to say in response! If the situation is anything like it is in China, then these companies and the universities will play a large role in providing the regime with a pool of talent from which to draw their cyber troops from—to find skilled staff to work on their infrastructure and systems.

3. To what extent is the Iranian regime self-reliant in terms of producing censorship/surveillance technology? Why is that?

Somewhat self-reliant in terms of on-going maintenance and the manpower needed to keep such systems running, but also heavily dependent upon global TNCs who provide the base infrastructure for such censorship regimes.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

Very large. Most of the technologies and infrastructure used by repressive regimes around the world is provided by transnational corporations, e.g. Siemens, Cisco.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I'm not sure that any regional form of governance can necessarily have a lot of impact, even if the willingness to impose restrictions was there. The unfortunate reality is that these companies operate in a global capitalist system, which places profit before anything else.

Hence, we have national governments preaching the benefits of internet freedom and decrying censorship while doing nothing at all to rein in such corporations or even speak out against them, because to do so would contravene the dominant profit logic, and therefore might impact negatively upon their political popularity. There is a lot of discursive hypocrisy going on in this respect.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

I really don't know any holistic data of the top of my head, but from what I do know/can make out, proxies and other firewall-circumvention tools would be the most commonly used technologies, and these are not just used by cyber-activists *per se*, but by many people/citizens. I think these tools are very practical, and in the same vein—and related to—the use of SNSs, great for promoting solidarity and co-ordination using platforms which might otherwise be unavailable. I think these kinds of technologies are also very important for disseminating news and information not just amongst Iranians within Iran, but to the rest of the world, so we can see what is going on, and thus exert pressure for change either indirectly or directly.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

My perception is that a lot of the tools being used by citizens and activists within repressive regimes all over the world are coming from technological activist groups primarily located in less repressive environments, who presumably have greater freedom in terms of developing and distributing these tools in the first instance. In this sense, there is an interesting political-economic alignment between the transnational/global power structures of both control and resistance: the infrastructures of both censorship/surveillance and its circumvention are coming from—largely—Europe and North America. This is not to say that Iran and other countries do not contribute at all in terms of providing the infrastructure/knowledge behind these flows, but my perception is that the majority of the tech and expertise on both sides of the struggle is coming from geopolitical centres/cores.

Dr. Ulises Mejias (24 Sep 2012)

1. Where do you place a) social networking and b) politically motivated hacking attacks in the online power struggle between the regime and cyber-activists in Iran?

Social networking can be a tool for organising activism and disseminating information, but it is not as directly confrontational as politically motivated hacking attacks.

If we are to agree with Ethan Zuckerman's Cute Cats theory of social media and activism, then the fact that people use social networking services to produce both political and non-political—cute cats—content can make this practice a) harder to censor, b) accessible to a broader audience than hacking attacks, and c) safer. This last point, however, is debatable in the case of Iran, where the government has at its disposal the same tools other governments have to monitor, track, and block online activities, but is willing to use them more overtly to stifle dissent.

2. What is the contribution of the government/IRGC-owned companies and institutions (i.e. universities) to the development of the Iranian regime's censorship/surveillance infrastructure?

I am not that familiar with the Iranian case, and everything I know is from secondary sources, as I have not conducted any primary research myself related to this area. However, from what I know, it sounds like it is no different from other cases in the sense that you have the confluence of academic research interests, corporate interests and government interests.

I think it would be difficult to find cases of military technologies and counter-insurgency technologies anywhere in the world that have not emerged as a result of the marriage of these three interests. Again, the case of Iran might represent a more extreme example in the sense that these are technologies developed to oppress Iranian citizens, as opposed to the citizens of other nations. But let's not forget that Iran's censorship/surveillance infrastructure was developed, in part, with the help of Western corporations like Nokia and Siemens.

4. What is, if any, the role of foreign, particularly European, telecommunications technology companies such as Nokia-Siemens Networks (NSN) in the repression of cyber-activists in Iran?

The case of Iran—along with others like China, Egypt, Libya, etc., where corporations have helped governments repress dissidents—demonstrates that capitalism trumps any ideals that European or US governments might profess to have about promoting democracy in the world. These governments are only slightly less responsible than the corporations, because they have been promoting policies of corporate deregulation that allow the companies to do what they are doing. But this is nothing new, as the case of IBM collaborating with the Nazis demonstrates.

5. How do you think international legislators (e.g. the European Parliament) can address the above issue through policy?

I understand some governments are beginning to formulate legislation that would control the export of technologies that can be used for censorship and surveillance. But the effectiveness of this approach remains to be seen, as the technologies that can be used for repression are, ironically—or not—the same ones that can be used for marketing.

6. What are the main anti-censorship/surveillance methods used by Iranian cyber-activists? How common/practical are such solutions?

I don't know enough about the specifics to answer this, but from what I understand, these are technologies developed not just for the Iranian context, but for worldwide application.

7. What are the main sources behind the development of the anti-censorship/surveillance software currently used by Iranian cyber-activists?

Again, I can't talk specifics, but it seems to me that it's mostly coming from a global but decentralised hacker community.

8. How do you differentiate the 'local' and 'expat' Iranian cyber-activists' role in the power struggle with the regime? Do you find gender/age to be a determining factor?

I don't know enough about the Iranian context, but if it's the same as in the rest of the world, I think we can assume that the expat community is mostly responsible for disseminating information about the movement, and that the use of social media by local cyber-activists is limited but focused and effective.

Western Technology Export Control Policy References

Dual-use Export Controls in the EU

Available at:

<http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls>

Lists of Items Prohibited for Export to and Import from the Islamic Republic of Iran

Available at:

<https://www.un.org/sc/committees/1737/exportimport.shtml>

US

Commerce Control List Categories: Telecommunications

Available at:

http://www.bis.doc.gov/index.php/forms-documents/doc_view/444-category-5-part-1-telecommunications

Glossary of Terms

Assembly of Experts is a parliament-like body of Muslim clerics directly in charge of the assignment (and possible removal) of the Supreme Leader, as well as monitoring his conduct.

Arab Spring is a popular phrase created in reference to the chain of pro-democracy movements taken place in Arab countries (Tunisia, Egypt, Libya, Yemen, Bahrain and Syria) since December 2010.

Basij is an Iranian paramilitary militia organisation with extra-judicial powers in an array of sensitive issues ranging from inland security to foreign policy.

Bonyads are tax-exempt, often oversized non-petroleum business firms subsidized by the regime, said to be responsible for about 20 per cent of Iran's GDP.

Clicktivism is a type of online activism focused on the application of advertising techniques to joining and defending a socio-political cause.

Color Revolution is a media-driven concept referring to a range of civil movements, which have taken place mainly in the post-Soviet Union and Balkan states since the year 2000, which has also been extended by some commentators to certain phases of the Arab Spring.

Cyber-activism refers to the use of ICTs in facilitation of promoting a socio-political cause through online techniques to help deliver certain types of information to a large [and otherwise unreachable] number of audiences.

Cyber-activist Innovation System (CIS) is a term coined by this research, which refers to an interconnected network of computer-literate, pro-democracy, online activists focused on counter-censorship ICT innovations.

Cyber Warfare refers to a set of online techniques used by a variety of individuals and groups ranging from criminals to political dissidents to disrupt and destabilise the networks and services run by (or supporting) the opposing force.

Digital Divide is the (often) class-based inconsistency in different individuals'/groups' extent of connectivity to the online world and the services it offers across a given society.

Distributed Denial of Service (DDoS) describes ICT-based attacks aimed to make an online network temporarily inaccessible to its potential users.

Diffusion of Innovations is a scholarly theory initially developed by Professor Everett Rogers in 1962, which endeavours to explain how and why innovation processes spread in a given country.

E-democracy refers mainly to the use of ICTs in (and by) democratic states to facilitate political processes.

Expediency Discernment Council is an assembly of veteran politicians and clerics appointed directly by the Supreme Leader, which seeks to resolve potential disagreements between Majlis and the Council of Guardians. It also functions as a consultant to the Supreme Leader in matters of national security.

Green Movement of Iran refers to a civil movement born in June 2009, following an allegedly rigged presidential election leading to the appointment of Mahmoud Ahmadinejad to presidency for a second term, during which the protestors demanded his replacement with Mir Hossein Mousavi, the statistically rightful winner of the polls.

Guardian Council is a 12-membered committee as set by the Islamic Republic's constitution with many important duties ranging from the supervision of all elections to the approval of candidates to participate in them.

Hactivism is a term coined by Cult of the Dead Cow in 1996, which refers to the use of hacking (such as DDoS) attacks to uphold socio-political causes.

Information and Communications Technology (ICT) refers mainly to the integration of traditional communication techniques with online networks through cabled or cable-free connections.

Internet Censorship refers to the interception or prevention of private communications often (but not always) conducted by governments or their affiliated institutions.

Innovation System (IS) refers to the systematic flow of information among actors needed in order to transform ideas into tangible results.

Iranian Cyber Police (FATA) is an online-oriented division of the Iranian police founded in January 2011.

Islamic Republic of Iran Broadcasting (IRIB) is a regime-subsidised Iranian corporation in control of all broadcast media.

Islamic Revolutionary Guard Corps (IRGC) is a giant, powerful organisation of nearly 130,000 specialised personnel and parallel to Iran's military, which specifically aims to ensure the compatibility of all the regime's general endeavours with the 'core principles' of Shiite Islam.

Majlis is Iran's equivalent of a Western parliament.

Mobile Phone Jamming is a technique used to disrupt cell phone signals across a given geographical area.

National Innovation System (NIS) refers to the flow of technological information among people, enterprises and institutions, the collaboration among which reflects a given country's innovation robustness and powers.

National Iranian Oil Company (NIOC) is a government-owned corporation run (and owned by) Iran's Oil and Petroleum Ministry.

Netizen, or cyber-citizen, is a term referring to any individual or community keenly involved in online activities particularly those favouring human rights and free speech.

Network Society is a broad term referring to any changes made to social, political, economic, cultural, etc. trends in relation with the development of the ICTs.

Online Community is an unconventional kind of neighbourhood consisting of online citizens who share a specific (often socio-political) cause.

Online Ethnography, or virtual ethnography, refers to a set of qualitative, social research methods which aim to combine ethnography with progressive, online communication techniques.

Orange Revolution refers to an internet-reliant civil disobedience taken place in Ukraine from November 2004 to January 2005, which was ignited by an alleged fraud in the run-off stage of the 2004 Ukrainian presidential election.

Political Economy is a term rooted in 18th-century philosophy, concerned with the study of a given state's economy.

Press TV is a 24-hour rolling news network broadcast only in English and owned by the state-run Islamic Republic of Iran Broadcasting (IRIB). The channel has recently been taken off the air by various European satellite companies due to a number of professional misconducts.

Quds Force is a special unit of the IRGC, mainly focused on the organisation's foreign endeavours.

Radio Jamming refers to the intentional disruption of satellite communications through the broadcast of illegitimate signals also known as noise.

Samizdat is a term referring a form of subversive and dissident communication in the Soviet Union, involving the reproduction and circulation of the regime-censored publications through manual (as opposed to digital) techniques. It is often seen as equivalent to today's cyber-activism.

Science and Technology Studies (STS) is the study of the interplay between socio-political (and sometimes cultural) values and technological innovations across one or more geographical regions.

Slacktivism is a phrase rooted in words 'slacker' and 'activism,' referring to a set of feel-good (but not necessarily effective) measures known to be taken by (less dedicated) cyber-activists worldwide.

Social Construction of Technology (SCOT) is an STS theory arguing against technological determinism, introducing technology as the ultimate product of human choices/actions.

Social Determinism of Technology is a school of thought considering technological innovations to be an outcome of the sociological environment, in which they are developed.

Social Networking Services (SNSs) are online platforms aiming to enable conventional social relations among people favouring the same causes/interests.

Social Shaping of Technology (SST) is an STS model developed by MacKenzie and Wajcman in 1985 with a strong criticism for technological determinism, underlining the socio-political contexts influencing a nation's technological choices.

Sociology of Scientific Knowledge (SSK) is the study of the relationship between social processes and scientific activity.

Socio-technical Systems is an inter-disciplinary concept mainly referring to the interaction between existing technological infrastructure and human behaviour across a given society.

Supreme Council of Cultural Revolution (SCCR) is a hard-line assembly based in the holy city of Qom, the main duty of which is ensuring full alignment of all cultural and educational productions and services with the core teachings of Islam and free from any Western influences.

Supreme Council of Cyberspace (SCC) is an assembly chaired by the Iranian president and responsible for regulating the online sphere.

Supreme Leader of Iran is the Islamic Republic's most senior authority directly in charge of the armed forces and the judiciary, and with extra-judicial powers to modify or overrule any decisions made by the regime's lower-ranking officials, including the president.

Supreme National Security Council (SNSC) is a security-oriented, policy-focused assembly as demanded by the Islamic Republic's constitution, which aims to safeguard the regime in the matters of national security, defence and inland or foreign threats.

Technological Convergence is a term mainly referring to the union of formerly detached concepts such as sounds, images, text, etc., in a way that they closely interact and due to technological advancements made in the field of ICTs.

Technological Dystopianism is the belief that views technology as inherently evil and inevitably harmful to moral, humanistic principles.

Technological Realism refers to some STS scholars' efforts to establish a constructive balance between radical, deterministic (utopian and dystopian) insights to the relationship between technological innovations and society.

Technological Utopianism is the philosophy that technological innovations will ultimately result in an ideal world, where there will be no (or very little) pain and suffering left, and where human living standards will be extremely high.

Ukrayinska Pravda is a popular, pro-democracy Ukrainian online news website published in Ukrainian, Russian and English, which was launched by Georgiy Gongadze in April 2000.

Web 1.0 refers to the initial, static and non-interactive phase in the development of the web, where the webmaster held all the editorial powers and the reader was a merely passive consumer of the information and news.

Web 2.0 is a term coined by Darcy DiNucci in 1999, which refers to the later, dynamic, highly interactive and frequently improving version of the web designed with the aim to put the power in the hands of the users, transforming them from passive consumers to active, influential participants.